



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

MBA PROFESSIONAL REPORT

Department of Defense
Strategic and Business Case Analyses for
Commercial Products in Secure Mobile Computing

**By: Matthew R. O'Neal and
Joshua S. Dixon
June 2011**

**Advisors: Nicholas Dew
Cynthia Irvine
John Dillard**

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE June 2011	3. REPORT TYPE AND DATES COVERED MBA Professional Report	
4. TITLE AND SUBTITLE Department of Defense Strategic and Business Case Analyses for Commercial Products in Secure Mobile Computing			5. FUNDING NUMBERS	
6. AUTHOR(S) Matthew R. O'Neal and Joshua S. Dixon,				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Marine Corps Systems Command PG11, 2200 Lester Street, Quantico, VA 22134-6050			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this paper are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____ N/A _____				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) <p>The Department of Defense (DoD) lags behind commercial entities in terms of adopting mobile computing technologies. Commercial smartphones offer scalable solutions to meet requirements ranging from business functions to tactical operations; however, these solutions require considerations beyond those applicable to the commercial sector. This research identifies whether potential solutions may contribute to three objectives: 1) reduce the DoD's currently high device and service costs; 2) increase the DoD's smartphone functionality; 3) maintain or increase the level of security functionality available in commercial devices for DoD.</p> <p>A strategic analysis of the commercial mobile communications industry highlights the business drivers and motivations of industry participants. This information is used to identify the DoD's strategic options, which, in turn, serve as the basis of business cases for adopting future smartphone capabilities. Business case analyses compare proposed cost models with the cost models for current smartphone implementations.</p> <p>Results indicate growing strategic opportunities for the DoD to acquire more economical commercial handsets and more flexible network services. The business cases may potentially save billions of dollars over seven years—i.e., the estimated life cycle of cellular network equipment. Risk assessments demonstrate the strong potential for the proposed solutions to maintain handset functionality, security features, and network coverage.</p>				
14. SUBJECT TERMS secure mobile communications, commercial mobile industry, strategic analysis, five forces analysis, value network, business case analysis, mobile virtual network operator			15. NUMBER OF PAGES 204	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**DEPARTMENT OF DEFENSE STRATEGIC AND BUSINESS CASE
ANALYSES FOR COMMERCIAL PRODUCTS IN SECURE
MOBILE COMPUTING**

Matthew R. O’Neal, Lieutenant, United States Navy
Joshua S. Dixon, Captain, United States Marine Corps

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF BUSINESS ADMINISTRATION

from the

**NAVAL POSTGRADUATE SCHOOL
June 2011**

Authors:

Matthew R. O’Neal

Joshua S. Dixon

Approved by:

Nicholas Dew, Lead Advisor

Cynthia Irvine, Support Advisor

John Dillard, Support Advisor

William R. Gates, Dean
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

DEPARTMENT OF DEFENSE STRATEGIC AND BUSINESS CASE ANALYSES FOR COMMERCIAL PRODUCTS IN SECURE MOBILE COMPUTING

ABSTRACT

The Department of Defense (DoD) lags behind commercial entities in terms of adopting mobile computing technologies. Commercial smartphones offer scalable solutions to meet requirements ranging from business functions to tactical operations; however, these solutions require considerations beyond those applicable to the commercial sector. This research identifies whether potential solutions may contribute to three objectives: 1) reduce the DoD's currently high device and service costs; 2) increase the DoD's smartphone functionality; 3) maintain or increase the level of security functionality available in commercial devices for DoD.

A strategic analysis of the commercial mobile communications industry highlights the business drivers and motivations of industry participants. This information is used to identify the DoD's strategic options, which, in turn, serve as the basis of business cases for adopting future smartphone capabilities. Business case analyses compare proposed cost models with the cost models for current smartphone implementations.

Results indicate growing strategic opportunities for the DoD to acquire more economical commercial handsets and more flexible network services. The business cases may potentially save billions of dollars over seven years—i.e., the estimated life cycle of cellular network equipment. Risk assessments demonstrate the strong potential for the proposed solutions to maintain handset functionality, security features, and network coverage.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
I. INTRODUCTION.....	5
A. PROBLEM	5
B. RESEARCH QUESTIONS	6
C. METHODOLOGY AND ORGANIZATION.....	7
II. THE COMMERCIAL MOBILE COMMUNICATIONS ECOSYSTEM	11
A. INDUSTRY DESCRIPTION	11
1. Summary Description of Industry Participants.....	13
<i>a. Mobile Network Operators.....</i>	<i>13</i>
<i>b. Radio and Core Network Device Providers.....</i>	<i>13</i>
<i>c. Content Providers.....</i>	<i>13</i>
<i>d. Handset Manufacturers and Retailers</i>	<i>14</i>
<i>e. Handset Component Manufacturers.....</i>	<i>15</i>
<i>f. Operating System Providers.....</i>	<i>15</i>
<i>g. Application Providers.....</i>	<i>16</i>
2. Mobile Network Operators in Depth	16
<i>a. Mobile Virtual Network Operators.....</i>	<i>17</i>
<i>b. Mobile Virtual Network Enablers</i>	<i>21</i>
<i>c. Supporting Service Providers</i>	<i>22</i>
3. Market-Influencing Factors	22
4. Value Network.....	23
B. INDUSTRY ANALYSIS	24
1. Five Forces Analysis of Mobile Network Operators.....	26
<i>a. Threat of Entry.....</i>	<i>27</i>
<i>b. Supplier Power</i>	<i>28</i>
<i>c. Buyer Power</i>	<i>29</i>
<i>d. Threat of Substitutes</i>	<i>30</i>
<i>e. Rivalry.....</i>	<i>31</i>
<i>f. Factors Crossing Multiple Forces</i>	<i>32</i>
2. Five Forces Analysis of Handset Manufacturers	33
<i>a. Threat of Entry.....</i>	<i>34</i>
<i>b. Supplier Power</i>	<i>35</i>
<i>c. Buyer Power</i>	<i>36</i>
<i>d. Threat of Substitutes</i>	<i>37</i>
<i>e. Rivalry.....</i>	<i>37</i>
<i>f. Factors Crossing Multiple Forces</i>	<i>38</i>
C. INDUSTRY OUTLOOK	39
1. Mobile Network Operator Trends	40
2. Handset Manufacturer Trends.....	41
3. Security in the Mobile Communications Industry	44
<i>a. The Meaning of the Term “Security”</i>	<i>44</i>

	b.	<i>The Supply of Security in the Commercial Market</i>	46
	c.	<i>Potential Sources of the Gap Between DoD and Commercial Demand for Security</i>	50
4.		Potential Ways Forward.....	51
	a.	<i>Leverage MVNO Flexibility.....</i>	52
	b.	<i>Exploit Handset Manufacturers' Reduced Bargaining Power</i>	53
	c.	<i>Team With Large Corporations.....</i>	53
	d.	<i>Education</i>	54
III.		BUSINESS CASE ANALYSIS FOR SECURE COTS HANDSETS	55
A.		BASELINE ASSUMPTIONS	56
	1.	Total Cost of Ownership	56
	2.	Base Case Platform (SME PED).....	57
	3.	Proposed Platform (Commercial Device)	60
B.		COST.....	62
	1.	CDS Architecture Cost	62
	a.	<i>Manufacturer Perspective (Willingness to Buy).....</i>	62
	b.	<i>Platform Provider Perspective (Willingness to Sell).....</i>	63
	2.	Encryption Cost	65
	3.	Future Features Upgrades	66
	4.	Additional Costs.....	66
C.		BENEFITS.....	67
	1.	Flexible Demand.....	67
	2.	Reduced Risk of Handset “Jailbreak”	67
	3.	Classified Mobile E-Mail Cost Savings.....	68
	4.	General Productivity Increase	71
	5.	Reducing DISA Security Technical Implementation Guides Cost.....	74
	6.	COTS Option Value.....	76
D.		RISK.....	76
E.		SENSITIVITY ANALYSIS.....	78
F.		SUMMARY	82
IV.		BUSINESS CASE ANALYSIS FOR LEVERAGING MOBILE VIRTUAL NETWORK OPERATOR SERVICES.....	85
A.		BASELINE ASSUMPTIONS	85
	1.	Current DoD Contracts.....	85
	2.	Current DoD Procurement Trends for Wireless (Mobile) Services.....	87
	3.	Best Practices.....	90
	4.	Mobile Virtual Network Operator Model	92
B.		MVNO COST ANALYSIS.....	96
	1.	Customer Service, Sales, and Billing.....	96
	2.	Integrated Voice-Mail and Messaging Services Cost	98
	3.	Edge Network Hosting Cost.....	99
	a.	<i>Commercial Spectrum.....</i>	100

	b.	<i>Unlicensed Spectrum</i>	103
	c.	<i>Department of Defense Allocated Spectrum</i>	106
	4.	Commercial Grade Core Network Cost	111
C.		BENEFIT	112
	1.	Customer Service, Sales, and Billing.....	112
	a.	<i>Telecommunication Expense Management.....</i>	113
	b.	<i>Local Telecommunication Offices Capacity</i>	113
	c.	<i>Reduced Contracting Costs.....</i>	114
	2.	Integrated Voice-Mail and Messaging Services	114
	a.	<i>DoD SMS/MMS</i>	114
	b.	<i>Integrated Voice-Mail.....</i>	116
	3.	Edge Network	116
	a.	<i>Mobile Intranet (Data Side).....</i>	116
	b.	<i>Increased Signal Coverage</i>	117
	c.	<i>Added Competency for Operational Deployments.....</i>	117
	4.	Commercial Grade Core Network	117
	a.	<i>Mobile Intranet (Completely DoD-Owned Network).....</i>	117
	5.	General MVNO Benefits	119
	a.	<i>Realigning Incentives</i>	119
	b.	<i>Specialized Handsets.....</i>	119
	c.	<i>DoD App Store</i>	120
	d.	<i>Additional Security.....</i>	120
D.		RISK.....	120
	1.	Residual Vulnerabilities	121
	2.	Value of Information (Impact)	124
	3.	Risk Calculation	125
E.		SENSITIVITY ANALYSIS.....	126
V.		COMBINED BUSINESS CASE AND CONCLUSIONS	133
	A.	COMBINED BUSINESS CASE	133
	B.	CDS SMARTPHONES.....	136
	C.	MVNO AS A SERVICE	137
	D.	SUMMARY OF STRATEGIC OPTIONS	138
	E.	FUTURE WORK.....	138
	1.	Stratification of Values and Requirements of User Groups	139
	2.	Detailed Risk, Vulnerability, and Threat Analyses of Specific Proposed Architectures	139
	3.	Competency Requirement.....	139
	4.	Determine the Best Contracting Mechanism for Obtaining Wireless Devices and Services.....	140
	5.	Determination of DoD Wireless Use by Region	140
	6.	Quantify the Benefits of a Larger Feature Set	140
	7.	Cost of Spectrum.....	140
APPENDIX A.		RISK, THREAT, AND VULNERABILITY	141
	A.	RISK.....	141
	1.	Threat Actions.....	142

2.	Vulnerabilities	143
3.	Impacts.....	145
B.	MEASURING SYSTEM VULNERABILITY	145
APPENDIX B.	DOD WIRELESS CONTRACTS.....	147
A.	ELECTRONIC DATA SYSTEM CONTRACT TRENDS.....	147
B.	NATIONAL DEPARTMENT OF THE NAVY WIRELESS CONTRACTS TRENDS	148
C.	ARMY AIR FORCE BLANKET PURCHASE AGREEMENTS TRENDS	148
APPENDIX C.	MVNO COSTS.....	153
APPENDIX D.	MILITARY END STRENGTH AND PAY CHART.....	155
APPENDIX E.	SECURE MOBILE ENVIRONMENT PORTABLE ELECTRONIC DEVICE FEATURES.....	157
APPENDIX F.	DOD PROCUREMENTS BY AREA.....	159
APPENDIX G.	CELLULAR NETWORK ARCHITECTURE	161
APPENDIX H.	PRODUCTIVITY RECOVERY CHARTS.....	163
APPENDIX I.	IN-DEPTH RISK ASSESSMENT.....	167
A.	THREAT.....	167
1.	Natural Threats	168
a.	Service Abuse	168
2.	Interception, Electronic Tracking, and Obstruction	169
3.	Remaining Threat Actions	169
B.	VULNERABILITIES	169
C.	IMPACT AND OVERALL RISK	171
	LIST OF REFERENCES.....	173
	INITIAL DISTRIBUTION LIST	187

LIST OF FIGURES

Figure 1.	DoD Wireless Services (Cost)	2
Figure 2.	DoD Wireless Services (Current Versus Proposed).	3
Figure 3.	Mobile Communications Industry–Hierarchical Depiction.....	12
Figure 4.	Economic Depiction of a Market With an MNO (no MVNO), Showing Deadweight Loss.....	18
Figure 5.	Economic Depiction of a Market With Both an MNO and MVNOs at Economic Equilibrium.....	19
Figure 6.	Industry Value Network.....	24
Figure 7.	U.S. Mobile Network Operators’ Market share.....	26
Figure 8.	End-User Telecommunications Revenues	30
Figure 9.	Net Additions (Change in Subscribership) of Four Largest MNOs	31
Figure 10.	Difference in Value Captured by MNO and Handset Markets.....	37
Figure 11.	Total Wireless Subscribers, Total MNO Revenues, and the Growth Rate of Each.....	39
Figure 12.	Annual EBITDA Per Subscriber for Selected MNOs.....	41
Figure 13.	Handset Market Share of Smartphones and Feature Phones	42
Figure 14.	Average Smartphone Selling Price	43
Figure 15.	Desired Characteristics	55
Figure 16.	Total Cost of Ownership Options	57
Figure 17.	Sectera Edge Upgrade Cost (Millions)	60
Figure 18.	Cross Domain Solution Example.....	62
Figure 19.	Potential Cost Savings for Mobile Classified E-Mail.....	69
Figure 20.	Minimum Potential Cost Savings	70
Figure 21.	Productivity Recovery Potential (From Moro, 2007)	72
Figure 22.	Potential Cost Savings for an Increase in Productivity.....	73
Figure 23.	Minimum Potential Saving for Increase in Productivity	74
Figure 24.	DISA STIG Process (From Defense Information Systems Agency, 2010).....	75
Figure 25.	Cost of Antiquated Technology (Uniform Distribution [in U.S. Dollars]).....	80
Figure 26.	Expected Distribution of Subscribers Who Receive Productivity Increase.....	81
Figure 27.	Cost of Antiquated Technology (Gamma Distribution [in U.S. Dollars]).....	81
Figure 28.	DoD Cellular Procurements,,.....	88
Figure 29.	Breakdown of DoD Wireless Expenditures by Vendor.....	89
Figure 30.	DoD Wireless Demand	90
Figure 31.	Network Operators’ Coverage Maps for Fort Knox, KY	93
Figure 32.	GSM Worldwide Coverage.....	94
Figure 33.	MVNO Divided Services	95
Figure 34.	Wi-Fi Architecture	105
Figure 35.	Tethered Smartphone to Military Radio	109
Figure 36.	Smartphone Sleeve Concept	110
Figure 37.	Value of Life Equation (From Lakamp, McCarthy 2003).....	115
Figure 38.	Network Architectures	118
Figure 39.	Residual Vulnerabilities Graph.....	124

Figure 40.	Percentage of Risk for Each MVNO Approach.....	126
Figure 41.	Cost of MVNO Concepts.....	127
Figure 42.	Cost of MVNO Concepts at Lower Levels of Demand.....	128
Figure 43.	Cost of MVNO Concepts at Higher Levels of Demand	129
Figure 44.	Cost of MVNO Concepts (Risk and Lease Line Expense Not Included).....	130
Figure 45.	Cost of MVNO Concepts (DoD Forecasted Demand)	131
Figure 46.	Monthly Cost per User for Each MVNO Concept.....	131
Figure 47.	Cost Benefit Ratio per MNVO Concept (300K Demand)	134
Figure 48.	Cost per User for Each MVNO Approach.....	135
Figure 49.	Cost per User for Each Type of Access Point.....	135
Figure 50.	EDS Contract	147
Figure 51.	NDWC Contracts	148
Figure 52.	AAFBPA Contracts	149
Figure 53.	NDWC and AAFPBA Procurement Distribution	159
Figure 54.	2G/3G/4G Cellular Architecture.....	161
Figure 55.	Expected Productivity Savings for 300K to 700K Subscribers	165
Figure 56.	Expected Productivity Savings for 1 to 700K Subscribers.....	165

LIST OF TABLES

Table 1.	Range of Services From Reseller Through MNO.....	21
Table 2.	Example Standards for Suppliers of MNOs.....	28
Table 3.	Cost of Selected iPhone Components	36
Table 4.	Comparison of Selected Security Features in BlackBerry and SME PED Devices.....	47
Table 5.	Examples of Multilevel Handset Efforts.....	48
Table 6.	Manufacturer Option.....	63
Table 7.	DoD Acquisition Process Option.....	64
Table 8.	Operating System Common Criteria Categories.....	77
Table 9.	Productivity Savings for 300K to 400K Subscribers.....	78
Table 10.	Productivity Savings for 1 to 400K Subscribers.....	79
Table 11.	Device Comparison.....	83
Table 12.	Device Cost Benefit Comparison.....	83
Table 13.	Major DoD Cellular Service Contracts.....	86
Table 14.	Standard Fixed Commercial RAN Costs	101
Table 15.	Unlicensed Bands.....	103
Table 16.	DoDs Plan for Spectrum Reallocations Funds.....	108
Table 17.	Potential Cellular Core Network Cost	112
Table 18.	Residual Vulnerabilities (Network Vulnerability Given Threat Action).....	122
Table 19.	Value of Information (Impact).....	125
Table 20.	Common Criteria Evaluation Assurance Levels.....	146
Table 21.	FISC NDWC Contract Summary by Network Operator	150
Table 22.	NMCI EDS Contract Summary by Network Operator	151
Table 23.	AAFBPA Contract Summary by Network Operator	151
Table 24.	Revenue of Top Four MNOs	152
Table 25.	Typical MVNO Costs	153
Table 26.	Typical MVNO Capital Expenditure and Other Costs	154
Table 27.	Military End Strength and Pay for Each Service (From http://militarypay.defense.gov)	155
Table 28.	Distribution of Military End Strength by Hourly Pay Rate	156
Table 29.	Productivity Savings Estimates for Between 1 and 700K Subscribers.....	163
Table 30.	Productivity Savings Estimates for Between 300K and 700K Subscribers...	164
Table 31.	Evaluated Potential of Threat Actions (Example)	168
Table 32.	Vulnerability Metrics	170

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAFBPA	Army Air Force Blanket Purchase Agreement
ACC	Army Contracting Command
ARPU	Average Revenue Per User
BEA	Bureau of Economic Analysis
CCI	Controlled Cryptographic Item
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
CTIA	Cellular Telecommunications & Internet Association
CDMA	Code Division Multiple Access
CDS	Cross-Domain Solution
CLIN	Contract Line Item Number
DoD	Department of Defense
DON	Department of the Navy
DTS-W	Defense Telecommunications Services–Washington
DSAWG	Defense Information Assurance Security Accreditation Working Group
EBITDA	Earnings Before Interest, Taxes, Depreciation, and Amortization
EDS	Electronic Data Systems
FAR	Federal Acquisition Regulation
FCC	Federal Communications Commission
FISC	Fleet & Industrial Supply Center
FY	Fiscal Year
GDP	Gross Domestic Product
GOTS	Government Off-the-Shelf
GSGN	Gateway GPRS Support Node
HLR	Home Location Register
IDIQ	Indefinite Delivery Indefinite Quantity
IETF	Internet Engineering Task Force
ISUP	ISDN User Part
IT	Information Technology

ITEC4	Information Technology E-Commerce and Commercial Contracting Center
PC	Personal Computer
PP&E	Plant Property and Equipment
PSTN	Publicly Switched Telephone Network
LAN	Local Area Network
MILS	Multiple Independent Levels of Security
MLS	Multilevel Security
MSL	Multiple Security Levels
MMS	Multimedia Messaging Service
MNO	Mobile Network Operator
MVNO	Mobile Virtual Network Operator
MVNE	Mobile Virtual Network Enabler
MVNA	Mobile Virtual Network Aggregator
NAVSUP	Naval Supply Systems Command
NDWC	Nationwide Department of the Navy Wireless Contracts
NMCI	Navy Marine Corps Intranet
NVA	Network Value Analysis
NCRCC	National Capital Region Contracting Center
NPV	Net Present Value
O&M	Operations & Maintenance
OS	Operating System
RAN	Radio Access Network
R&D	Research and Development
SIP	Session Initiation Protocol
SDK	Software Development Kit
SGSN	Serving GPRS Support Node
SME PED	Secure Mobile Environment Portable Electronic Device
SMS	Short Message Service
SMSC	Short Message Service Center
TEM	Telecommunication Expense Management

VLR	Visitor Location Register
VMM	Virtual Machine Monitor
Wi-Fi	IEEE 802.11 Wireless LAN standard

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The authors would like to acknowledge the financial support of Marine Corps Systems Command, Product Group 11, Marine Air Ground Task Force Command and Control (MAGTF C2), for allowing the purchase of market research material under Contract number M6785410WRR0DP0.

LT O’Neal expresses his deep appreciation and love to his wife for her constant hard work and continual support. He is also especially thankful for his mom’s steadfast, positive encouragement. He thanks his advisors for their patience and guidance throughout the development process. Finally, a special thanks to Dr. Jim Suchan for his support and persistence in setting the conditions for this work to begin.

Capt. Dixon would like to thank his loving wife and kids for their understanding during long nights and constant support throughout the development of this paper. He would like to thank all the advisors for their assistance throughout the revisions and continuous questions—without their help, the paper might still be unfinished. Finally, he would like to thank John Gibson for his assistance in refining the larger picture and suggestions for tailoring the paper towards a broader audience.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The Department of Defense (DoD) has a clearly stated need for interoperable, affordable, innovative, and small form factor mobile communication devices. To date, however, the DoD has been unable to acquire a suitable device, or set of devices, that meets all of its needs. The DoD's unique requirements for supporting secure communications further increase the complexity of efficiently procuring the devices.

Currently, the defense services procure unclassified commercial handsets and network services in a fractured manner via various contracting vehicles. The inefficiencies found in these vehicles ultimately limit the DoD's mobile communications potential for both unclassified and classified communications. Although the existing vehicles for procuring secure communications are more centralized, the current government-only solutions also result in inefficiencies. The shortfalls in the current situation ultimately translate to imprudent cost allocations, either directly in actual dollars or indirectly through various means (e.g., decreased productivity or suboptimal technical capability).

The authors of this paper conducted strategic and business case analyses to identify a path toward achieving mobile communications solutions that meet the following criteria:

- 1) Reduce the DoD's high device and service costs,
- 2) Increase overall smartphone functionality for the DoD, and
- 3) Maintain or increase the level of security functionality available in commercial devices for the DoD.

The strategic analysis points out trends in market conditions that may allow the DoD greater leverage in acquiring suitable commercial handsets. Most notable among these trends are the apparent decreasing bargaining power of handset manufacturers and increasing opportunities for more flexible acquisition of mobile voice and data service (i.e., Mobile Virtual Network Operator [MVNO] opportunities).

Following the strategic analysis, business case analyses address the potential costs, benefits, and a limited set of security considerations for undertaking the following two efforts: (1) acquiring a commercial off-the-shelf (COTS) cross-domain solution (CDS) smartphone, and (2) implementing one of various MVNO business models to obtain network services. As illustrated in Figure 1, these analyses yielded the following conclusions:

- The current level of DoD spending for reoccurring wireless services is \$235M for FY2010 with a \$40M increasing trend. The current SME PED average annual total cost of ownership (including service) is \$4,100 per user (amortized over 2 years).
- Over seven years, DoD can potentially save \$1B (in current dollars) by implementing the most cost-beneficial MVNO.

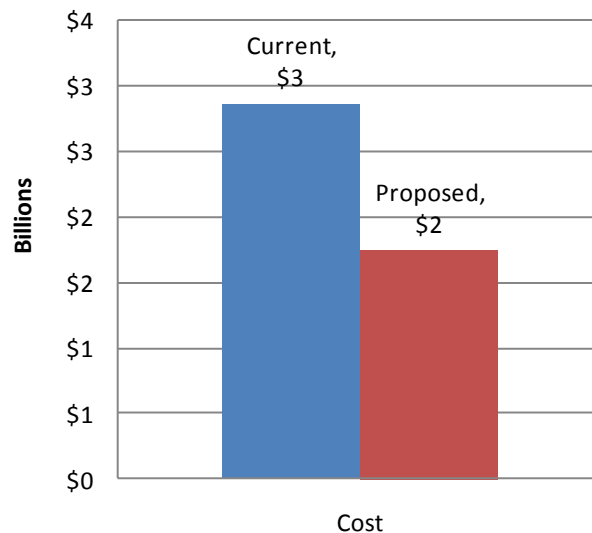


Figure 1. DoD Wireless Services (Cost)

In Figure 1, the blue bars represent the net present value (NPV) of costs for current DoD wireless services on the unclassified (e.g., BlackBerry) and classified (e.g., SME PEDs) domains. The proposed (red) bars represent the NPV of costs for the least costly MVNO approach.

Figure 2 presents only the costs in order to clearly illustrate the difference in each of the seven years. The numbers under the years indicate the total estimated demand for wireless services based on current DoD trends.

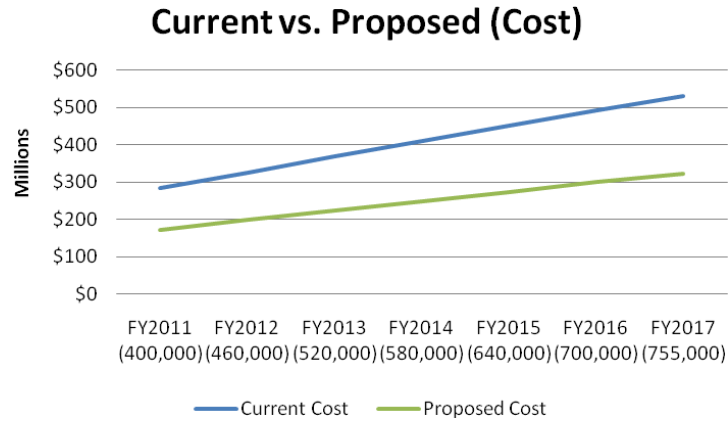


Figure 2. DoD Wireless Services (Current Versus Proposed).

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM

On 20 Oct 2009, the Director of Army Capabilities Integration Center, Lieutenant General Michael Vane, signed a memorandum for the Army Acquisition Corps, clarifying his intent for the capabilities set 13-14 (FY13-14 solution). The document states,

We strongly urge the development of an alternative that leverages the use of commercial technology at Company and below (Personal Digital Assistants [PDA], Blackberry, iPhone, etc.) for both Battle Command applications and communications and secure data only that needs to be classified as part of the transport system.

The document continued by outlining objectives for the proposed capability at each level of command: (i) across echelons—provide command and control capabilities to enhance situational awareness and reduce current communication short falls, (ii) battalion and above—reduce communications hardware footprint, (iii) company and below—increase response time by reducing end-to-end latency. The remaining paragraphs provide a more detailed outline of the Army’s specific goals for adopting the technology (Vane, 2009).

Later that year, 28 Dec 2009, the U.S. Army Vice Chief of Staff, General Peter Chiarelli, signed a memorandum stopping all acquisitions of communication devices without G-3/5/7 LWN/BC Directorate approval. The purpose of the order was to prevent purchase of ongoing noninteroperable communication devices. Over the past 8 years of the war, thousands of orders were submitted without any effort to maintain interoperability. He specifically stated, “We must encourage innovation, not stifle it, while ensuring it can be integrated within a consistent and affordable network strategy” (Chiarelli, 2009).

For the purpose of this paper, the point of referencing these documents is to highlight and validate the existence of a requirement for interoperable, affordable, innovative, and small form factor communication devices. Currently, multiple program offices within the Marine Corps and Army (MCSC PG-12 and PEO C3T) are actively

refining a capabilities development document in conjunction with their respective requirements offices (MCCDC and TRADOC) in an effort to acquire devices in line with these high-level directives. In addition to the acquisition efforts, multiple Broad Agency Announcements (BAAs) and Requests for Information (RFIs) (i.e., BAA W15P7T-08-R-P001, RFI CDID JTWCC, etc.) are posted in response to these continuing capability requirements. The ground elements of the military are poised to adopt cellular handset capabilities.

In the past, DoD acquisition processes failed to provide a solution because of unsupportable business cases for suppliers, or because of the length of the acquisition process. Because of the nature of DoD procurements, technologies tend to change during the acquisition process, resulting in sometimes deprecated and incompatible equipment by the time it is fielded. These are well-known problems that commonly occur during acquisitions of rapidly changing technologies.¹

The overall goal of this work is to identify potential solutions to facilitate the following outcomes for the DoD:

- Reduce the traditionally high cost of secure mobile devices, and reduce costs for network services
- Increase functionality in the form of handset capabilities and increased mobile network coverage.
- Maintain, and in some cases increase, the level of security of mobile communications in the DoD.

B. RESEARCH QUESTIONS

The research is inspired by the lack of military communication capabilities in comparison with the commercial industry. In the interest of leveraging COTS smartphones for military applications, the research described here analyzes the COTS smartphone industry and develops a business case for adopting future smartphone

¹ Refer to the September 2006 GAO report on Best Practices for a discussion of some issues. Report number GAO-06-883. Available from <http://www.gao.gov/>.

capabilities. The authors focus on identifying the current cost models and comparing them with various proposed models. Findings indicate that the DoD can acquire COTS solutions at lower costs than current Government Off-the-Shelf (GOTS) solutions without significantly increasing security vulnerabilities.

This research aims to answer the following questions:

- What are the potential costs and benefits of integrating secure COTS smartphone capabilities with existing military networks?
- Who are the participants in the mobile communications ecosystem and what drives their businesses?
- To what extent does the DoD require a separate infrastructure to support secure communications?
- What cost drivers are shaping the commercial smartphone market and will continue to drive them in the future? What are the cost drivers and models for the current Department of Defense (DoD) smartphones?
- What are potential costs to modify a COTS smartphone to meet the specifications required by DoD communication policies?
- What are the potential security benefits and risks of the various options for the DoD to obtain mobile computing capabilities?
- What benefits might be captured by making COTS smartphones available to a wider base of DoD users?
- What blend of cost, security, and performance will provide the most security functionality for the least cost?

C. METHODOLOGY AND ORGANIZATION

The following methods were used to gather and analyze data in support of answering the research questions:

- A network value analysis to identify and discern the relationships between industry participants.
- A five forces analysis to analyze the network services market and the handset market within the United States.
- Cost analyses to identify the costs of the current DoD solution, the base case, as well as those of other potential solutions.
- A high-level risk analysis of each potential solution to determine its security benefits.
- A comparison and sensitivity analysis of the costs and benefits of potential solutions to those of the base case will complete the cost-benefit analysis.

The following list describes the contents of the ensuing chapters:

Chapter II. A strategic analysis of the commercial mobile communications ecosystem aimed at identifying the participants and the factors that drive their business decisions. This chapter includes an assessment of the DoD's strategic options for leveraging the industry to obtain mobile computing capabilities.

Chapter III. A business case analysis of the acquisition of secure COTS handsets for DoD personnel.

Chapter IV. A business case analysis of the potential reorganization of the DoD's strategy for the use of a Mobile Virtual Network Operator model to obtain mobile network services.

Chapter V. A summary of the DoD's strategic options, a summary and list of the potential benefits of COTS smartphone and network service business cases, and a discussion of potential future work.

Additionally, appendices as listed in the table of contents are included to elaborate on background and supporting information or provide data used in the analyses. Finally, government-only addenda containing sensitive but unclassified information are internally maintained and are available upon request.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE COMMERCIAL MOBILE COMMUNICATIONS ECOSYSTEM

The commercial mobile communications ecosystem consists of a global industry encompassing multiple subindustries and markets that work together to deliver mobile voice and data services to consumers. Analysts often refer to these subindustries as regional industries, and they are generally separated by geographic boundaries. One can further segment these subindustries into their contributing parts. For instance, network operators and handset manufacturers make up the two major subcomponents of any regional mobile communications industry. However, the dynamics within industries in different regions can vary significantly due to a multitude of factors such as government regulations and consumer tastes. Therefore, when necessary for simplicity and accuracy, this chapter focuses its description and analysis on the mobile communications industry in the United States.

A. INDUSTRY DESCRIPTION

The mobile communications industry exists to connect the mobile consumer with the existing telecommunications infrastructure (both the publicly switched telephone network [PSTN] and the Internet). This merging of technologies serves as a source of complexity in the market structure, and it influences the growth of the industry. Due to this dynamic, ranking providers of the various services is very difficult. In these cases, examples of current firms are provided.

A fragmented, but highly interconnected industry has materialized to deliver the voice and data capabilities that mobile users demand. The major entities consist of those who perform the following activities:

- Develop and manage the infrastructure.
- Develop and provide mobile handsets to users.
- Provide content (data) for mobile users to access.

Figure 3 depicts the industry structure as a hierarchy meant to illustrate the general positioning of major market participants. It begins with the single global industry at the top, regional network operator subindustries in the next layer, and then the various market participants in the lower layers. This depiction identifies the participants and their general alignment, but it only hints at the intricacies of the markets. For instance, government regulation and technical standards and protocols are shown in the margins to acknowledge the fact that those forces affect operations and evolution of the industry. The value network, presented following the description of industry participants, focuses on displaying interactions between firms.

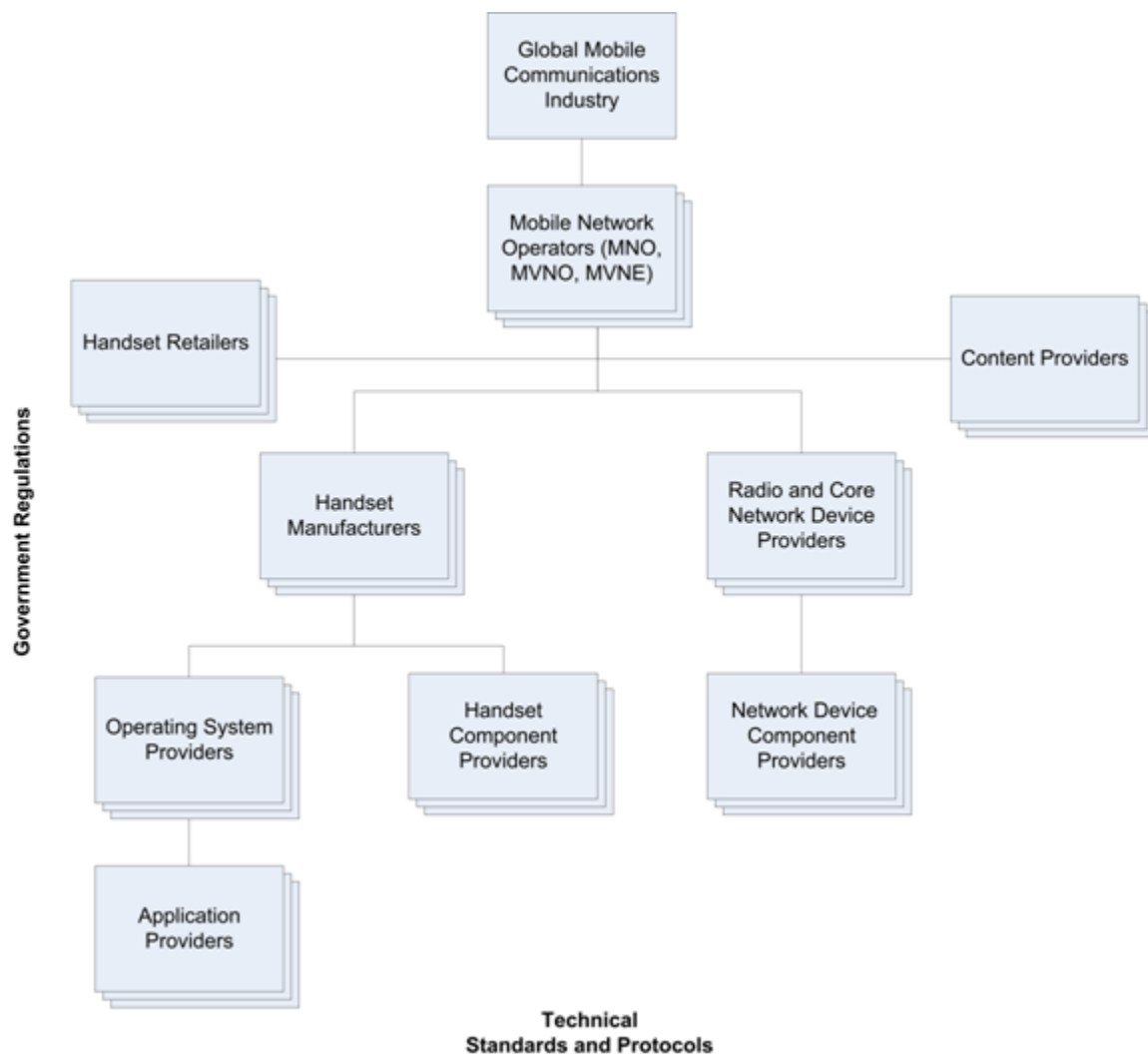


Figure 3. Mobile Communications Industry–Hierarchical Depiction

1. Summary Description of Industry Participants

The following paragraphs offer descriptions of the industry participants illustrated in Figure 3. In addition to a basic description, the paragraphs provide examples of specific firms performing those functions.

a. Mobile Network Operators

Mobile Network Operators (MNO) essentially act as the gateway for users to access the capabilities, products, and services located within the PSTN and Internet. They invest in providing, leasing, and managing mobile networks. MNOs earn revenue by selling service to consumers (including operators who resell services). AT&T, Verizon, Sprint, and T-Mobile represent the top MNOs in the United States (Smith, 2010).² A more detailed description of MNOs follows this summary of participants.

b. Radio and Core Network Device Providers

The radio access and core network device providers specialize in designing, fabricating, and selling the actual hardware components that make up the mobile network. They provide this hardware to MNOs who connect and operate the equipment along with machine-to-machine capabilities that are essential to an MNO's ability to offer quality services to customers. Network device providers may specialize in either radio or core network equipment, or they may be diversified between the two. They may also operate in other industries that require similar technology. Some examples of radio and core network providers include Ericsson, Nokia Siemens Networks (joint venture between Siemens AG and Nokia), and Motorola Solutions, Inc.³

c. Content Providers

Content providers develop and make content (e.g., ringtones, wallpaper, and location-based information) available to users via either a network operator's portal (e.g., T-Mobile's T-zones) or the Internet. They provide this service to the users, but their

² Based on company descriptions available from Hoover's Company Records database (2011, March 1).

³ Ibid.

revenue may come either from the network operator or directly from the user. Additionally, this category of industry participants includes what McNally et al. (2007) described as content aggregators. These aggregators interface between content providers and network operators (providing a many-to-one or many-to-many relationship) to facilitate content formatting for presentation to users via operators' portals (McNally et al., 2007). A content aggregator may maintain a network operator's portal or a portal of its own, which users access via a handset. Increasingly, one can describe any company with an online presence as a content provider. Specific content providers include the following companies: Hands-On Mobile, Inc.; Digital Chocolate, Inc.; and Glu Mobile, Inc.⁴ The companies, Zed Worldwide, Digital Bridges, and Motricity, represent content aggregators.⁵

d. Handset Manufacturers and Retailers

Handset manufacturers provide users with the means for accessing content, or connecting with one another, via the mobile network. These firms earn revenue by selling handsets to MNOs and retail businesses who, in turn, sell those handsets to consumers. Examples of retail businesses include Radio Shack, Walmart, and Target. Handset manufacturers invest in research and development, and they perform the integration and engineering necessary to build handsets from hardware and software obtained from various suppliers. The industry separates handsets into multiple categories based on their capabilities. The terms *smartphone* and *feature phone* appear most commonly used to describe the majority of mobile devices currently available. CTIA-The Wireless Association® (CTIA, 2010a), defined smartphones as “wireless phones with advanced data features and often keyboards ... [and the] ability to better manage data and Internet access” (para. 6). Synthesizing this definition with that of others, this project defines smartphones as mobile cellular handsets that support high-level operating systems and are capable of running advanced third-party applications (Pyramid Research, 2009; Llamas & Stofega, 2010; Smith, 2010). Given no authoritative definition for feature

⁴ Based on company descriptions available from Hoover's Company Records database (2011, March 1).

⁵ Ibid.

phone, one can regard a feature phone as a handset that provides voice and data capabilities via a simplified user interface with limited potential for third-party applications. The leading mobile phone manufacturers in the United States are Nokia, LG, Motorola, and Samsung (Datamonitor, 2010c). The leading smartphone manufactures, according to Global Industry Analysts (2010), include Research in Motion (RIM) and Apple, who commanded a combined 75% of the market in 2008. Other competitors include Palm (acquired by HP in 2010), HTC, Samsung, and Nokia (Global Industry Analysts, 2010).

e. Handset Component Manufacturers

Handset component manufacturers build the electronic hardware that resides within the handsets. This category of firms consists of a wide variety of businesses that produce items ranging from handset casings to antennae to microprocessors. These components must meet communication specifications for the network they access, and they must integrate into the overall design of the handset. Therefore, producers of these components must interface with both handset manufacturers and applicable wireless standards-developing bodies. Among leading component manufacturers, Qualcomm is one of the most well-known semiconductor companies. Its competitors consist of Broadcom, Texas Instruments, and Freescale Semiconductor.⁶

f. Operating System Providers

Although the operating system (OS) can be considered a handset component, it plays a unique role. Software firms—synonymous with platform providers—develop the OS to interface with all of the other components (e.g., screen, keyboard, memory, etc.). They market their products directly to end-users as well as handset manufacturers. Because the OS exists partly to optimize management of system resources, platform providers must work with handset manufacturers to ensure interoperability with the hardware. These firms invest in software development and

⁶ Based on company descriptions available from Hoover's Company Records database (2011, March 1).

interoperability with handset hardware. They earn software-licensing revenue from handset manufacturers. The following list contains OSs that led the global smartphone market in terms of units shipped in 2009: Symbian, BlackBerry, Windows, and iPhone OS (MarketsandMarkets, Inc., 2010).

g. Application Providers

Logically, applications run at a higher and less-privileged layer than the OS (i.e., the applications reside above the kernel and middleware). Applications on mobile phones perform specific usability-enhancing functions for users beyond those that the OS provides organically. Providers of applications must work with OS vendors, or at least have access to OS application programming interfaces, to ensure compatibility with the OS. Applications may be prepackaged with operating systems (e.g., games), suggesting a perceived advantage of combining the two complementary products. Alternatively, an end user may add (i.e., install) third-party applications to the device. Smartphones such as iPhone and BlackBerry, and increasingly others, leverage the latter case. In this model, an application provider can range from a major corporation to an end user. For example, *Time* magazine maintains a list of the top 50 iPhone applications for 2011 by category: Games (Angry Birds, Scrabble, Plants v. Zombies, etc.), On the Go (Kayak, Yelp, Word Lens, etc.), Lifestyle (e.g., Amazon, Epicurious, Mixology), Music and Photography (e.g., Mog, Pandora, Sound Hound), Entertainment (e.g., Netflix, IMDb, ESPN Scorecenter, etc.), and Social (Facebook, Twitter, Google, etc.).⁷

2. Mobile Network Operators in Depth

Jaspers, Hulsink, and Theeuwes (2007) described the MNO function as both network management and service provision. Traditionally, the MNO provides all of these capabilities as a vertically integrated firm, but fairly recent developments have created space for others to participate in the process. MNOs remain the central participants; however, Mobile Virtual Network Operators (MVNO) and Mobile Virtual Network Enablers (MVNE) can augment the MNO. In the United States, an MNO obtains a

⁷ List found on *Time Magazine* website: www.time.com.

license from the government to utilize a given frequency band in a given area. The MNO then acquires network infrastructure and institutes operational (managing the network), business (customer interaction), and marketing (supporting marketing campaigns and sales activities) support systems (McNally et al., 2007). These three systems are sometimes referred to as simply the operational support system (OSS), and their existence sheds light on the wide range of activities the MNO function encompasses. The notion that a firm builds its businesses around a single core competency (e.g., managing radio networks or customer support) supports the case for existence of other specialist firms like the MVNO and MVNE.

a. Mobile Virtual Network Operators

To an end user, MVNOs provide the same services that MNOs provide; however, the term virtual indicates that, in reality, some MNO functions are normally abstracted away. CTIA-The Wireless Association (2010b) defined an MVNO as “a company that buys network capacity from a network operator in order to offer its own branded mobile subscriptions and value-added services to customers” (para. 11). In essence, the industry generally views an MVNO as a network operator that does not own spectrum. Note, however, that exceptions may exist due to continual innovation of the business case.

(1) *The Economic Business Case for MVNO*. McNally et al. (2007) asserted that the MVNO business model has been driven by the following three strategies:

- Segmentation-driven strategies: MVNOs may help MNOs reach different market segments by providing more targeted marketing.
- Network utilization-driven strategies: Through targeted marketing, an MVNO may help an MNO utilize excess capacity.
- Product-driven strategies involving marketing to customers who have specialized service requirements. For example, provision of service centered on handsets that contain simple interfaces and large buttons.

Economic theory helps illustrate one scenario in which an MVNO adds value to the industry. Consider a market where the incumbent MNO operates a

mobile network serving a large majority of the consumer base but has no intention to offer service (advertise) to the remaining underserved consumers who are not willing to pay as much. As illustrated in Figure 4, the MNO charges a service price (P_1 on the y-axis) that it determines will maximize its marginal benefit. It will not lower the price because the marginal cost of doing so outweighs the marginal benefit. Q_1 , on the x-axis, indicates the quantity of service that consumers demand based on the price. The shaded area indicates an inefficiency called deadweight loss (DWL) resulting from this arrangement. In this case, the DWL represents remaining network capacity, or bandwidth, that goes unused. The MNO has already incurred the cost of leasing the spectrum, but it reaps no benefit from the unsold capacity. Similarly, some consumers demand service, but they are unwilling to pay the price at P_1 . Thus, the DWL represents the value of the MNO's unsold capacity combined with the consumers' unmet demand.

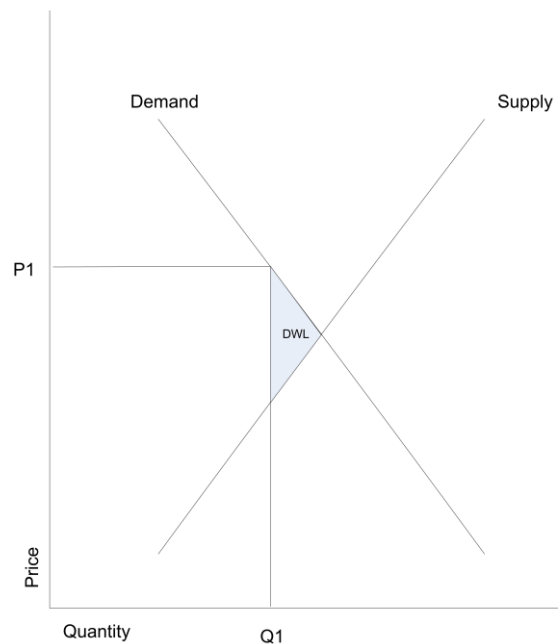


Figure 4. Economic Depiction of a Market With an MNO (no MVNO), Showing Deadweight Loss

Given the aforementioned conditions, an MVNO can enter this market, offer a price that the underserved consumers are willing to pay, and tailor the service to those consumers' values. In this ideal scenario, all parties gain in the following ways:

- The MNO earns revenue on the previously unused capacity that it sells to the MVNO.
- Previously underserved consumers obtain service.
- The MVNO earns a profit by providing mobile services to a select group more efficiently than the MNO.

Figure 5 illustrates the resultant market at equilibrium with a higher quantity of service (Q_e) provided at an overall lower price (P_e). This example represents one of many cases, presented here to help explain the continuing presence of MVNOs in the industry.

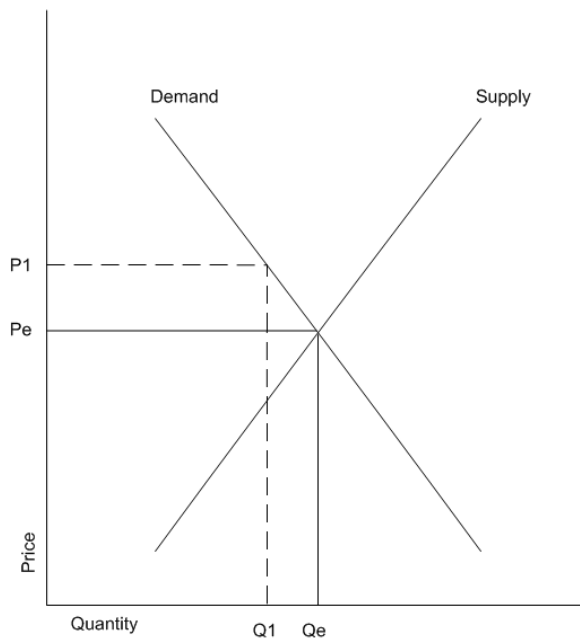


Figure 5. Economic Depiction of a Market With Both an MNO and MVNOs at Economic Equilibrium

In this example, the value of the MVNO to its host MNO lies in the fact that it targets a specific user base (i.e., possibly, but not necessarily, a niche

market) that differs from the host MNO's user base, thereby allowing the MNO to gain revenue from otherwise unused capacity. The model protects the MVNO from competing with its host MNO; however, this model can result in competition between the MVNO and other MNO competitors. In this case, the MVNO essentially acts as a fighting brand where its low price competition combines with the host MNO's differentiation to take market share from competing MNOs or MVNOs.⁸ Such a strategy is part of a broader pattern of industry specialization and change.⁹

(2) *The MVNO Continuum*. As previously stated, any operator that provides services to consumers, but does not own spectrum, may be referred to as an MVNO. This definition is quite broad, given the breadth of requirements to provide basic mobile service. Jaspers et al. (2007) have distinguished between types of MVNOs based on the extent to which they control their own resources. The term service provider (SP) refers to resellers, enhanced service provider (ESP) describes those who also offer services such as voice-mail, and full MVNO indicates firms who perform more network management services (managing core network functions, etc.) (Jaspers et al., 2007; H. White, 2010).

Table 1 illustrates the range of services available to an MVNO by listing a subset of operator-provided services and indicating which type of operator will provide that service. The MNO column is included in the table to serve as a point of reference.

⁸ For a discussion of fighting brands, see: "Multiproduct quality competition: fighting brands and product line pruning," by Johnson & Myatt (2003) in *American Economic Review* 93, no. 3, 748–774.

⁹ For further discussion, see Geroski & Vlassopoulos (1991) and Jacobides (2005).

	MVNO			MNO
Service	Reseller (SP)	ESP	Full MVNO	
Sales	✓	✓	✓	✓
Marketing	✓	✓	✓	✓
Customer Service	✓	✓	✓	✓
Billing	✓	✓	✓	✓
Provisioning (issue SIM)		✓	✓	✓
Voice-mail service		✓	✓	✓
Messaging Services (SMS*, MMS**, etc.)			✓	✓
Manage Core Network			✓	✓
Manage Radio Access Network (RAN)				✓
Own Spectrum Rights				✓
*SMS: short message service				
**MMS: multimedia messaging service				

Table 1. Range of Services From Reseller Through MNO¹⁰

b. Mobile Virtual Network Enablers

According to McNally et al. (2007), a MVNE “provides infrastructure and services to enable MVNOs to offer services” (p. 38) to consumers. The MVNE fills the gap between the services the MVNO chooses to provide and those that the MNO will maintain. Consider, for example, a firm aspiring to function as a SP (i.e., provide sales, marketing, customer service, and billing) under a MNO that does not wish to provide the intermediate services (i.e., those listed under ESP and full MVNO in Table 1) to enable the SP’s business model. A MVNE may provide a service to the SP by offering provisioning and messaging services, for example, on behalf of the SP. This relationship allows a MVNO the flexibility to start its business at any point in the MVNO continuum, focusing on the set of services that allows it to maximize its profit while potentially developing competency in offering more services. Over time, if supported by its business model, the MVNO can take over services from the MVNE.

Extending the MVNE model, an entity called the Mobile Virtual Network Aggregator (MVNA) has recently joined the European industry. This type of firm does

¹⁰ Adapted from data presented by Jasper et al. (2007) and White (2009). Note: while the terms SP and ESP do not appear globally standardized, they do seem well understood in the European industry.

not currently appear to have a strong presence in the United States, but it may expand into the U.S. market, so it is briefly described here. A MVNA provides services similar to those of a MVNE. Additionally, the MVNA “purchases mobile airtime in bulk from the partner mobile operator, adds its service platform and wholesales this airtime to multiple MVNOs” (A. White, 2010). The U.K. company x-Mobility represents an example MVNA.¹¹

c. Supporting Service Providers

McNally et al. (2007) have drawn attention to the existence of underlying service providers that enable the value-added services hosted on MNO networks. These firms are not depicted in the diagrams, but are worth mentioning as enablers of the MNO’s functions. Radio Access Network (RAN) providers such as American Tower Corporation and Crown Castle International Corporation construct base station towers, lease the equipment to MNOs, and may provide operational support.¹² While they act as network device providers, these firms also participate in providing the MNO function. Concordantly, within the core network, specialized firms may provide messaging capabilities (e.g., voicemail, SMS, and MMS messaging), Internet Protocol (IP) subsystem, telephone number clearinghouse, and other services. Core network providers may include the provision of some of these services along with their infrastructure equipment, but standalone providers also exist in this submarket. In the current work, we consider these entities part of the MNO business—they are mentioned here to shed light on a submarket existing beyond the scope of this analysis.

3. Market-Influencing Factors

A description of this industry is incomplete without consideration of the forces that contribute to its current state and evolution. Additionally, Figure 3 includes government regulation and standardization. Beyond general business regulations,

¹¹ X-mobility claims to provide the services of MVNO, MVNE, and MVNA. See <http://www.x-mobility.com/mvna-mobile-virtual-network-aggregator/>.

¹² The Mergent Online database (2008) described American Tower Corporation as an owner and operator of wireless communications sites; and Crown Castle, listed as a competitor, has a similar business description.

governments can significantly influence the actions of private and public businesses. In the United States, the Federal Communications Commission (FCC) enforces the telecommunications stipulations in the Telecommunications Act. The FCC's management of the commercial electromagnetic spectrum shapes the industry because all activity centers on the ability to transmit and receive radio signals. The FCC assigns and manages spectrum rights through licenses.

Likewise, technical standards and protocols (e.g., standard hardware interfaces or Code Division Multiple Access) influence the design and construction of devices as well as how they are used. Standards place limits on either the type or method of hardware production, but they also help to foster interoperability between components manufactured by different vendors. They encourage and enable rapid and wide fielding of the complex technologies at the heart of this industry. The influence of both of these forces is clarified in the industry analysis.

4. Value Network

Figure 6 illustrates the Value Network diagram resulting from the above discussion of industry participants. Each square represents a market participant. Lines represent some relationship between them, and the arrows indicate a positive flow of value or benefit. For instance, the double arrow on the link between handset manufacturers and network operators indicates that each entity benefits from the relationship (i.e., value flows in both directions). The analyses of the MNO and handset manufacturer markets provide further insight into these relationships.

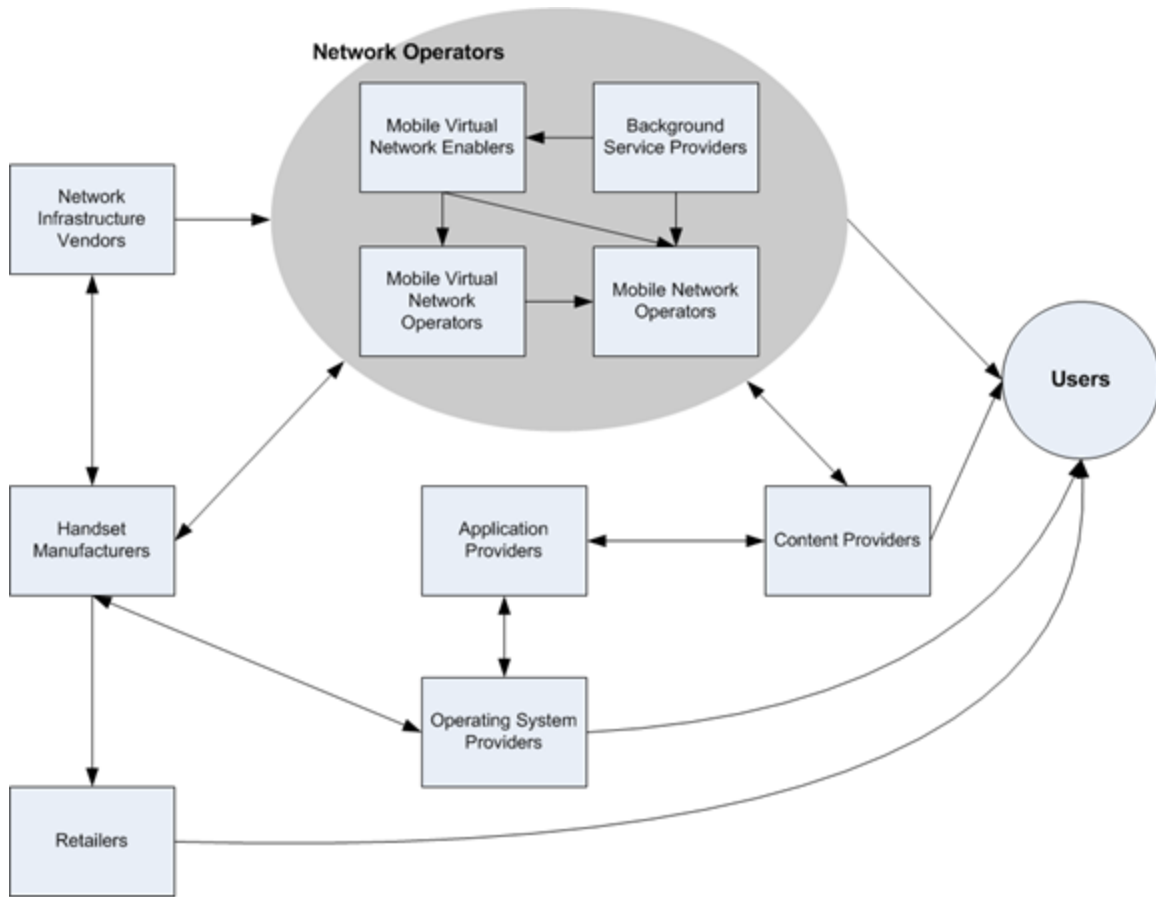


Figure 6. Industry Value Network¹³

B. INDUSTRY ANALYSIS

This industry analysis employs Porter's five forces analysis technique to illuminate the drivers of industry profitability (Porter, 2008). Due to the complex set of interrelationships between entities, two separate analyses were conducted: one from the perspective of MNOs, and the other from the handset manufacturers' perspective. This separation follows the argument that industry functions exist in two broad segments. One segment focuses on content-related services and applications, and the other focuses on network infrastructure and edge devices (Sabat, 2003). The MNOs act as the hub of

¹³ Developed using methods discussed by Christensen (1997) and Peppard & Rylander (2006). This figure was influenced by similar diagrams presented by Peppard & Rylander (2006), Lin (2003), and Whalley and Li (2002).

content-related services and applications, and the handset manufacturers provide the edge devices. Infrastructure developers and vendors serve as the suppliers and enablers of these two markets.

The following list describes Porter's five forces:¹⁴

- Threat of Entry: A high threat of entry by new firms tends to limit profitability through downward pressure on prices. Analysis mostly consists of consideration of the barriers to entry.
- Supplier Power: The bargaining power of suppliers can affect prices, costs, and the actions of industry participants. Powerful suppliers tend to limit profitability by seizing a greater share of the value of products and services.
- Buyer Power: Powerful consumers can limit profitability by demanding lower prices.
- Threat of Substitutes: Porter describes substitutes as ever-present but easily overlooked. A high threat of substitutes limits profitability.
- Rivalry: Indicative of competition and taking many forms, a high degree of rivalry limits industry profitability.

Porter (2008) has also considered the following four factors that intersect multiple forces: industry growth rate, technology and innovation, government (regulation), and complementary products or services. Two goods are complements if an increase in the price of one good leads to a decrease in demand for the other (Mankiw, 2006)—consumer demand for both goods is synchronized. Additionally, and along the same lines of complements, this industry is susceptible to network effects that may impact multiple forces. This phenomenon links a product's value with the number of consumers using it—that is, buyers place greater value on a particular product as the product's user base increases (Katz & Shapiro, 1985). Discussion of these factors is included at the end of each analysis.

¹⁴ As described by Porter (2008).

1. Five Forces Analysis of Mobile Network Operators

Overall, the U.S. MNO market appears highly attractive and profitable for incumbents. MNOs face a very low threat of entry, they are strong compared to buyers and suppliers, substitutes are limited, and rivalry remains tempered by a high growth rate and high technological innovation.

The fact that only a few MNOs control the majority of the market share (Datamonitor 2010b) serves as strong evidence supporting the notion that MNOs reside in a generally comfortable position. Figure 7 illustrates the market share of the leading MNOs, showing that these four firms control 89% of the market. The strong positioning of these market leaders gives them an advantage in seizing new opportunities that result from the high industry growth rate. The market value growth rate was 7.7% between 2005 and 2009 (Datamonitor, 2010b).

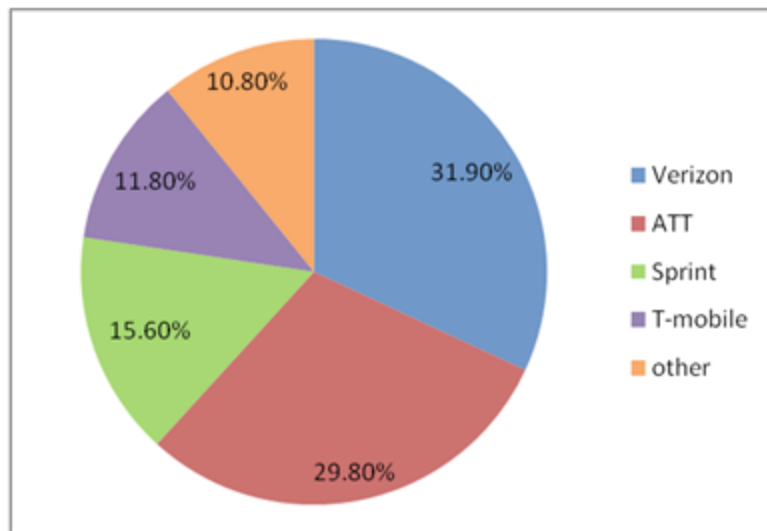


Figure 7. U.S. Mobile Network Operators' Market share¹⁵

The following paragraphs assess each force, identifying the driving factors, and assigning a score of either low, moderate, or high.

¹⁵ From Datamonitor (2010b).

a. Threat of Entry

Entry barriers determine the threat of entry into the market. The predominant barriers for this market include capital requirements and regulation (i.e., the way the FCC allocates spectrum and interprets and enforces telecommunications policy). The threat of entry into the industry as an MNO is assessed as low. The driving forces are discussed in the ensuing paragraphs.

(1) *Capital Requirements.* The data from the 700 MHz cellular auction that closed in March 2008 illustrate the large capital requirements for entering the MNO market. The FCC awarded approximately one thousand licenses for approximately \$19B (FCC, n.d.).

(2) *Regulation.* In its auction 73 fact sheet, the FCC (2008) lists specific permissible operations to which MNOs are constrained during the ten-year license period. For example, licensees holding Cellular Market Area (CMA) and Economic Area (EA) licenses must meet benchmark criteria for providing cellular coverage to specific amounts of the population in their license area. They must file construction notices and supporting documentation to show compliance with the benchmarks. Noncompliance results in a two-year reduction of the license term. While the FCC levies these requirements to ensure that licensees develop and provide services with the spectrum they acquire, these requirements also increase firms' barriers to entry by increasing legal and capital requirements.

The FCC also takes actions that encourage competition and result in lowered barriers to entry. It offers bidding credits, in the form of either a 15% or 25% discount on winning bids, to small and very small businesses respectively. A small business has a three-year average annual revenue of between \$15M and \$40M, and a very small business has a three-year average annual revenue of less than \$15M). The commission also incentivizes development on federally recognized tribal lands by offering additional bidding credits to those firms bidding for spectrum on those lands. Notwithstanding these mitigations to high entry barriers, the largest bidders still

maintain a healthy competitive advantage. The data show that the two largest U.S. MNOs, AT&T Mobility and Verizon Wireless, own winning bids worth nearly \$16B (82% of the sum of all winning bids) in auction 73.

This assessment does not include the entry of subindustry participants such as MVNOs. The threat of entry for these entities is increasing due to FCC policy,¹⁶ but MVNOs by definition lack the resources to affect the business viability or profitability of MNOs.

b. Supplier Power

The main suppliers to MNOs include radio access and core network providers, messaging providers, content providers, and various other service providers. Supplier power is assessed as low due to standardization, an abundance of suppliers, and substitutes for content providers. Table 2 lists examples of standards for RAN providers, core network providers, and content providers.

RAN	Core Network Providers	Content Providers
UMTS	SMS	MNO Portal
GPRS	MMS	WAP
HSPA+	SS7	IP

Table 2. Example Standards for Suppliers of MNOs¹⁷

Standardization reduces entry barriers for the network and service supplier markets, and it reduces suppliers' opportunities to differentiate from competitors. Suppliers' inability to differentiate is an indicator of low supplier power (Porter, 2008). This situation results in larger numbers of suppliers and, therefore, higher competition as the supplier base increases. Supplier power decreases as the combined size of suppliers increases relative to the size of MNOs. This relationship exists because an MNO can use

¹⁶ See http://wireless.fcc.gov/licensing/index.htm?job=secondary_markets.

¹⁷ After McNally et al. (2007) and 3GPP, <http://www.3gpp.org>.

the competition between suppliers to induce lower prices. More suppliers equates to more leverage for an MNO. These phenomena reduce the power that suppliers can wield over MNOs.

In evaluating content providers, McNally et al. (2007) asserted that the power of content providers decreases as users gain options for accessing content. For instance, as Table 2 implies, users have the option of accessing content directly via the Internet instead of having to transit an MNO portal, content aggregator, or specially formatted WAP page. The existence of HyperText Markup Language (HTML) browsers on handsets greatly increases the amount of content a user can reach and simultaneously reduces the power of content providers and aggregators relative to that of MNOs.

c. Buyer Power

General categories of buyers include residential, corporate (both small business and large enterprise), and government customers. The market position of the MNOs, previously presented in Figure 7, represents a significant factor in limiting buyer power. The high rate of growth and the large number of consumers also drive buyer power downward; therefore, buyer power is assessed as low.¹⁸

The CTIA (2010c) reported the number of mobile subscribers as 292M in the second quarter of 2010. It also reported that the average local monthly bill was \$47.47, translating to \$570 per year. Individually, each customer lacks the power to affect the revenue of even T-mobile, the lowest-earning of the top four MNOs in 2009. As for larger customers, the DoD had a total budget of \$693B (DoD, 2011) and spent approximately \$221M¹⁹ on mobile services in 2009. This dollar value equals about 1% of T-mobile's 2009 revenue of \$21.5B. Assuming the DoD represented one of the largest—

¹⁸ Porter (2008) states that the existence of few buyers indicates high buyer power, thereby implying that a large number of buyers indicates low buyer power.

¹⁹ Refer to Chapter IV for details on DoD spending.

if not the largest—mobile service purchasers in 2009, one may conclude that no single large-volume purchaser can exert enough economic influence to affect the margins of MNOs.

d. Threat of Substitutes

The threat of substitutes is assessed as low due to the high industry growth rate and sustained MNO revenues. Porter (2008) defined a substitute as an item that “performs the same or a similar function” (p. 84) as the item in question. In this case, the function performed involves mobile access to voice communications and data services. The following set of substitutes provided by Sabat (2003) applies: IEEE 802.11 (Wi-Fi) voice and data technology, wireline (e.g., digital subscriber line [DSL], cable, and PSTN) voice and data technology coupled with personal computer (PC) functionality, and cordless telephones. None of these substitutes offers the same range of capabilities as an MNO’s services, indicating a reduced threat. Additionally, the high industry growth rate indicates a low threat of substitutes. In terms of revenue, the FCC has reported decreases in wireline access accompanied by increases in wireless access (“Trends in Telephone Service,” 2010). Figure 8 illustrates this trend, supporting the assertion that users value wireless service over those of substitutes, especially wired services.

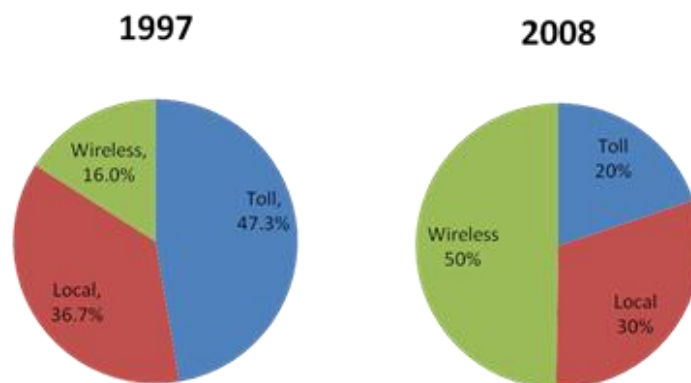


Figure 8. End-User Telecommunications Revenues²⁰

²⁰ After FCC (2010a).

e. Rivalry

This assessment considers the effect of rivalry on profitability. The large market share controlled by the four largest MNOs indicates reduced rivalry. Furthermore, Figure 9 displays their net additions—change in subscribership—showing that only Sprint has lost market share in recent years while the other three gained more subscribers. Given this situation, the intensity of rivalry is assessed as low. The following list provides the conditions under which rivalry is most intense, according to Porter (2008):

- Competitors are numerous or have roughly equal size and power.
- Slow growth of the industry.
- High exit barriers.
- Competitors are highly committed to the business, especially beyond economic performance.
- Firms are inhibited from reading each other's signals.

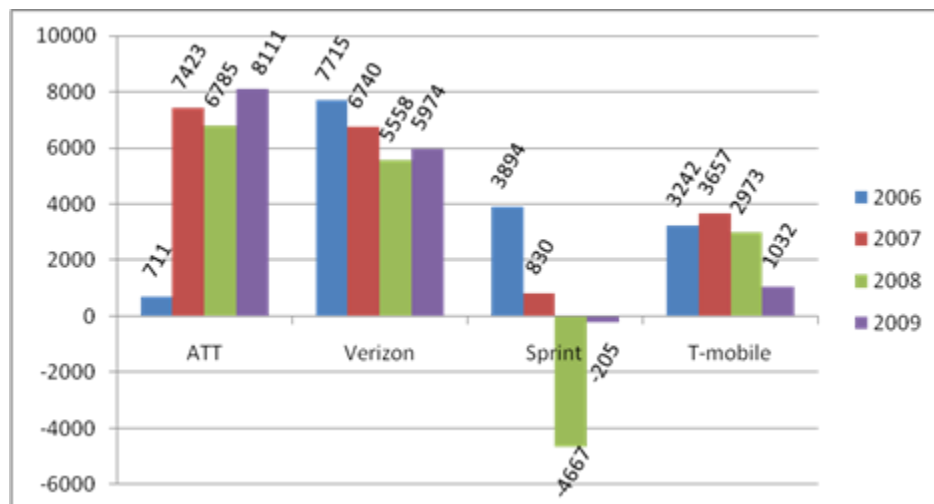


Figure 9. Net Additions (Change in Subscribership) of Four Largest MNOs²¹

As the industry market share indicates, the major competitors are not numerous, and even the four largest firms have widely varying size and power. Similarly, the industry's 7.7% Compound Annual Growth Rate (CAGR) demonstrates that the

²¹ From FCC (2010b).

growth rate is not slow. While the high entry barriers tend to increase the exit barriers (due to a firm's drive to recoup its investment), all of the leading MNOs retain sufficiently diversified business structures to effect lowered exit barriers for themselves. The United States Telecommunications Report (2010) has reported the following information: AT&T has its roots, and remains deeply involved, in the fixed line telecommunications industry; Verizon Wireless is 45% owned by The U.K.'s Vodafone (suggesting international diversification) and participates in the fixed-line market; Sprint was founded as a fixed-line company in 1898 and remains involved in that market; T-mobile is owned by the globally diversified international company Deutsche Telekom. In March 2011, AT&T announced its acquisition of T-mobile.²² There are no apparent indications that any MNOs participate in the market for noneconomic reasons or have trouble reading each other's signals.

Datamonitor (2010b), among others, has reported intensifying competition; however, Porter (2008) has noted that "Competition on dimensions other than price—on product features, support services, delivery time, or brand image, for instance—is less likely to erode profitability because it improves customer value and can support higher prices" (p. 86). Therefore, a high degree of competition on a single dimension other than price does not necessarily equate to high rivalry; and the data indicate that while MNOs compete aggressively for increased market share and revenue, this competition does not have a negative effect on their profitability.

f. Factors Crossing Multiple Forces

As is apparent in the above analysis, the high growth rate of 7.7%, coupled with high entry barriers, helps solidify the position of incumbents. New technology requires innovation, which, in turn, requires capital and expertise to manage its high risk. Furthermore, this constant innovation is aimed at providing the highly valued capabilities of increased mobility and higher data rates. Incumbents gain and maintain market share through this cycle of investing capital, accepting the high risk of innovation, and providing valuable new services to consumers who demand those services.

²² Press release available from <http://www.att.com/gen/landing-pages?pid=6080>.

The FCC restrictions on MNOs act as a significant barrier to entry, and they help shelter the incumbent MNOs from new entrants. In the year 2000, the FCC instituted its Secondary Markets Initiative²³ to foster the development of secondary (reseller) markets for radio spectrum. However, this initiative only reduces the barriers for entry into the reseller and MVNO markets. The regulatory barriers to entering the market as an MNO remain unaffected by this initiative.

Porter (2008) stated that “the need to attract complements can raise barriers to entry” (p. 87). This assertion, coupled with the complex nature of the MNO business, indicates significantly high entry barriers because successful MNOs must work with many providers of complementary products and services to attract and retain customers. Those providers include handset manufacturers, voice-mail service providers, and content providers, among others. This situation supports the conclusion that this market remains attractive to incumbents while unattractive to new entrants.

Vertical integration—one entity offering all services—represents a commitment that may attract more customers, however, partial integration via partnerships and joint ventures may suffice to increase an MNO’s market share.²⁴ To this end, MNOs may use relationships with providers of complements, or they may offer specific services, as parts of strategies to leverage network effects. Verizon’s offer of unlimited calls and mobile messaging to other Verizon wireless customers provides an example of such a service.²⁵ The network effects of the mobile market magnify the resulting increase in customer switching costs—i.e., costs incurred by who those switch to a different service provider. Increased switching costs reduce buyer power.

2. Five Forces Analysis of Handset Manufacturers

This analysis is limited to the smartphone market, since that platform is more appropriate for providing robust mobile computing capabilities. The participants in the broader U.S. handset market appear moderately well positioned with smartphone

²³ See http://wireless.fcc.gov/licensing/index.htm?job=secondary_markets.

²⁴ Katz and Shapiro (1985) discuss vertical integration.

²⁵ Based on information provided at <http://www.verizonwireless.com/b2c/splash/mobiletomobile.jsp>.

manufacturers less so. The fast-paced nature of the market represents the major challenge to the strength of incumbents and market leaders. Also, communication standards and protocols, plus the physically limited space for differentiation, allow firms to compete in multiple global regions. These facts facilitate entry of new firms, and tend to decrease incumbents' overall power.

According to Datamonitor (2010c), the top handset manufacturers for all handsets include Motorola, Samsung, LG, and Nokia. Global Industry Analysts, Inc. (2010) reported the top U.S. smartphone makers in 2008 as RIM (55% market share), Apple (20% market share), and others (25%—including Palm, HTC, Nokia, Samsung, etc.). This disparity between leading manufacturers of different phone types illustrates the continual shift from old technology to that which is newer and more capable.

a. Threat of Entry

The threat of entry is assessed as moderate. This market requires relatively high capital and a high degree of expertise to design, manufacture, and integrate handset components for commercial use. Branding also raises barriers to entry and helps solidify the positions of some incumbents such as RIM and Apple.

The market research firm, Pyramid Research (2009), reported the smartphone market share in quarter 3 of 2009 as follows:

- RIM: 50%
- Apple (iPhone): 24%

Note that both RIM and Apple vertically integrate their handsets with in-house produced OSs. They also have strong brand images as leaders in the corporate user group (RIM) and innovation (Apple). The remainder of the market share remains fragmented between nonvertically integrated manufacturers. This situation suggests a

lower threat of entry; however, new entrant opportunities are buoyed by the overall market growth rate of 5.8%²⁶ and the decreasing cost of the smartphone.²⁷

Finally, the actual entry of new firms signals decreasing entry barriers. Companies producing electronics similar to smartphones may diversify into producing smartphones themselves—Apple’s entry into the market with the iPhone serves as an example (Datamonitor, 2010c). Other examples include Dell and Acer’s planned entry into the market (Business Monitor International [BMI], “Company Profiles,” 2010), and Hewlett Packard’s acquisition of Palm (Edwards, 2010).

b. Supplier Power

Smartphone suppliers reside in one of two groups: those supplying components common to all handsets, and the suppliers of components unique to smartphones. Common component providers have low power because, as previously asserted, standardization yields larger numbers of providers. The providers of the more valuable features that are unique to the smartphone, such as the operating system and touch screen, wield much more power than other providers because they provide capabilities highly valued by end users. Therefore, supplier power is assessed as moderate.

Table 3 presents selected data from an iPhone 3G component teardown showing the differences in component costs. Higher cost components indicate a higher value, which, in turn, suggests higher bargaining power for suppliers of those components.

²⁶ See Datamonitor’s (2010c) reported market value CAGR.

²⁷ Multiple sources including MarketsandMarkets (2010) and Global Industry Analysts, Inc. (2010). Exemplar data provided by The NPD Group (2009).

Component	Cost (\$)	% of total
Improved Touch Screen	\$ 20.00	12.0 %
Display	\$ 20.00	12.0 %
Application Processor	\$ 13.50	8.0 %
HSDPA* Digital Baseband	\$ 15.00	9.0 %
1Gbit SDRAM — Mobile DDR	\$ 5.00	3.0 %
WLAN** chipset	\$ 4.00	2.5 %
RF Transceiver	\$ 4.25	2.5 %
Total Bill of Materials (BOM) Costs (Direct Materials Only)	\$ 164.00	100 %
*HSDPA: High-Speed Downlink Packet Access **WLAN: Wireless Local Area Network		

Table 3. Cost of Selected iPhone Components²⁸

c. Buyer Power

The buyers of smartphones consist of MNOs and third-party retail businesses, who, in turn, sell phones to end users. As discussed earlier, MNOs represent the most powerful entities in the industry, and they tend to buy phones in large quantities. These facts suggest a strong potential for high buyer power. The handset does maintain a key position as the user's entry point to access the network and reach content. Marketing directly to end users, entering into partnerships, and entering exclusive agreements with MNOs may help smartphone manufacturers maintain some of their power. The recent Microsoft-Nokia partnership illustrates these points.²⁹ This partnership allows Nokia to differentiate its phones from those running Apple and Android OS, and Microsoft gains exclusivity with an overall leader in the handset market. It is unclear whether marketing and partnerships significantly affect the behavior of buyers. Given these facts, buyer power is assessed as high.

In both its phone and services industry profiles, Datamonitor (2010b; 2010c) reported the 2009 market values for services (operators) and phones (handsets) as \$152.6B and \$10.4B, respectively. Based on this data, Figure 10 displays the percentage of the combined total that each market captures. This comparison of market values

²⁸ From Carson (2008).

²⁹ As reported in *Microsoft and Nokia Partner on Smartphone Future* by Ionescu, D. on February 11, 2011. Available from <http://www.pcworld.com>.

illustrates the ability of MNOs to pull more value from the industry, and from partnerships, than handset manufacturers. These data support the conclusion that buyer power is high.

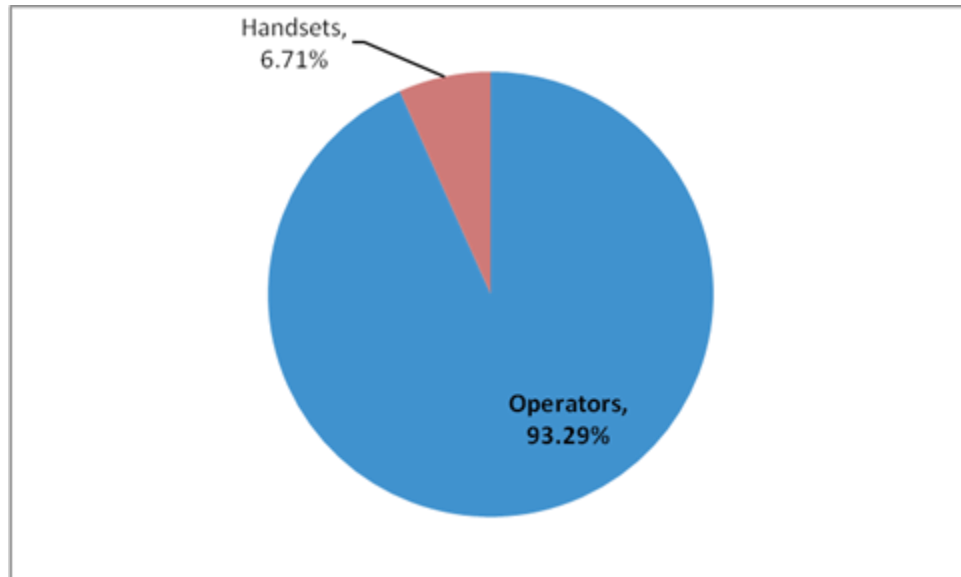


Figure 10. Difference in Value Captured by MNO and Handset Markets³⁰

d. Threat of Substitutes

The threat of substitutes for smartphones is similar to the threat of substitutes for MNOs. While a wide range of devices can perform a subset of smartphone functions, no devices currently provide the same set of capabilities. Similar devices include tablet PCs, personal digital assistants, pocket PCs, netbook PCs, and 2-way radios. Some of these devices, such as laptops, may also act as complements, since users tend to own both a handset and a laptop (Datamonitor, 2010c). Due to the smartphone's unique set of capabilities, the threat of substitutes is assessed as low.

e. Rivalry

Based on Porter's (2008) criteria for highly intense rivalry, listed in the above MNO analysis, rivalry for this industry is assessed as low.

³⁰ After FCC (2010b).

Competitors are relatively few, with RIM and Apple capturing nearly 75% of the market value. Although the field is growing, this data indicates low rivalry for the present.

The industry continues to grow in volume, value, and technological capability. MarketsandMarkets (2010) reported that smartphones represented 9% of total phone sales in the first quarter of 2008, increasing to 23% by the end of 2009, and projected to continue on that trend through 2014. Finally, there are no indications that any manufacturers participate in the market for noneconomic reasons or have trouble reading each other's signals.

f. Factors Crossing Multiple Forces

Similar to the MNO market, the high technological and economic growth rate increases market attractiveness for incumbents. However, the reduced entry barriers for smartphones also make the market appear attractive for new entrants. The growth rate increases innovation and drives competition on quality and capability higher, but rivalry for those innovation leaders remains low—that is, the competition does not significantly affect their margins. Furthermore, the high rate of technological change increases market profitability.

The existence of complementary products and services can significantly impact the success of a handset. For example, if a handset manufacturer partners with a strong MNO, licenses a highly valued OS, or delivers its own complementary services (e.g., RIM's enterprise services), that manufacturer could enjoy greater sales. Nokia's strategy to bolster its business sales by partnering with Microsoft epitomizes this argument.³¹ The possibility of these alliances increases entry barriers and competition because it induces manufacturers to partner with both sellers and buyers who offer complementary products and services. Additionally, network effects of the market can increase the magnitude of the effects of these scenarios.

³¹ See press release, Nokia and Microsoft announce plans for a broad strategic partnership to build a new global ecosystem. Available from <http://press.nokia.com>.

C. INDUSTRY OUTLOOK

Based on market trends and data presented in the Five Forces analyses, this section estimates impending changes to the industry and explores the areas that the DoD may best leverage to maximize performance, security, and cost savings.

While the number of wireless subscribers has been steadily increasing since 1985, the rate of that growth (measured in percent change) has been steadily decreasing (CTIA, 2010c). Figure 11 depicts this situation. These trends indicate that both increases in subscribers and increases in revenues are approaching zero, serving as an indicator of market saturation. Reduced growth yields reduce opportunities for differentiation, lead to increased rivalry, and create a higher likelihood of price competition in the markets that benefit from subscriber growth.

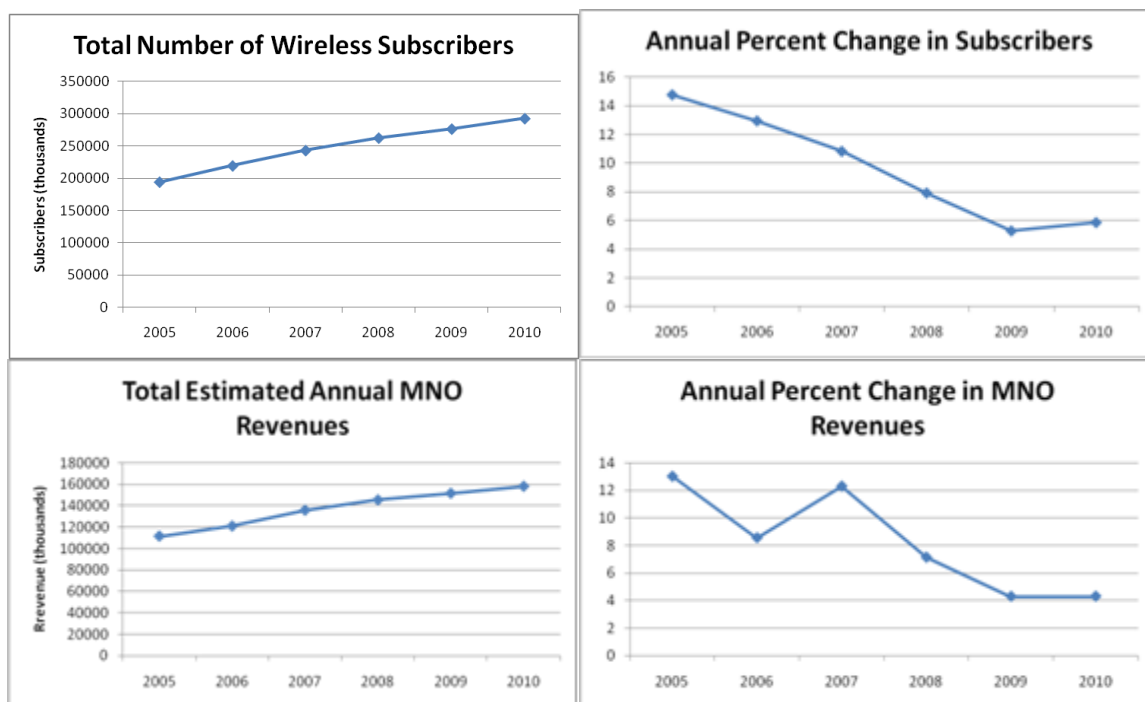


Figure 11. Total Wireless Subscribers, Total MNO Revenues, and the Growth Rate of Each³²

³² From CTIA (2010). Note: the estimated MNO revenues are based on midyear revenue reports. Charts depict only recent data here.

1. Mobile Network Operator Trends

Mobile Network Operators are the most powerful industry participants. They require products and services from multiple firms in order to conduct business, but they still manage to capture a large amount of the industry value, as shown when comparing MNO revenues to handset manufacturer revenues (Figure 10). MNOs will likely maintain their strong relative position due to no signs of changing government regulation regarding spectrum management, thereby keeping the entry threat low. Government efforts have encouraged growth in secondary markets (i.e., the secondary markets initiative) and rural markets (i.e., the Broadband Technology Opportunities Program [BTOP]).³³ These incentives, coupled with MNOs' willingness to support the MVNO business case, will support the continued growth of the MVNO, MVNE, and MVNA markets. BTOP Funds are not necessarily for cellular work, but could spark niche market growth in rural areas for either cellular or substitute technologies.

The efforts to develop faster and more capable networks (e.g., LTE and WiMax), coupled with standards organizations' efforts to proliferate standards, contribute to the continued consolidation of wireless technologies.³⁴ Network equipment costs are also decreasing (Morgan Stanley, 2009). As more operators adopt increasingly more capable radio access and core network technologies, they will gain capacity to provide better services to users, but they will lose the ability to differentiate on that facet. This situation will contribute to increased rivalry. MNOs will likely seek increased revenues on unused capacity via MVNOs. Continued rivalry could induce MNOs to resort to price competition, sacrificing profit margins to retain customers.

Although price competition between MNOs represents a logical possibility, its likelihood is reduced by the fact that these trends have so far had no appreciable effect on MNO revenues. Figure 12 displays the earnings before interest, taxes, depreciation, and amortization (EBITDA)—an indicator of profitability—over the past five years for selected MNOs. This data shows that even the profits of smaller MNOs—Leap and U.S.

³³ BMI ("Market Data," 2010). Also see BTOP website at <http://www2.ntia.doc.gov/>.

³⁴ The FCC (2010b) discusses the development of this situation.

Cellular in this case—have either remained constant or increased. Their ability to sustain profitability shows that MNOs have so far been able to find ways to maintain operating efficiency to make up for decreasing revenues. In addition, they have avoided price competition by offering increased quality or services (e.g., 4G technology).

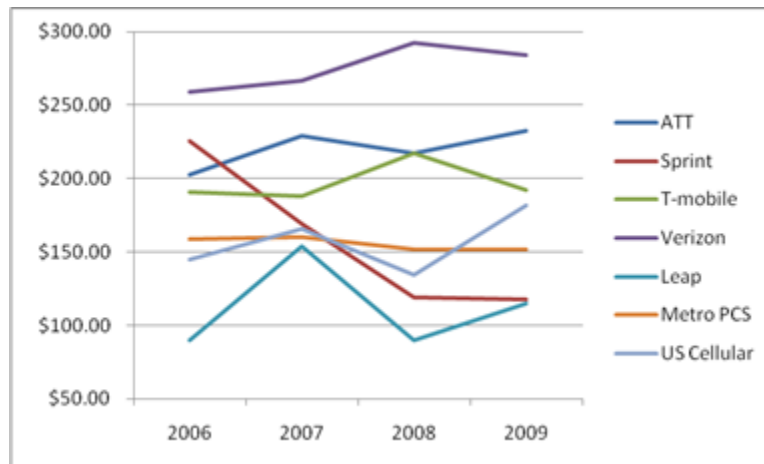


Figure 12. Annual EBITDA Per Subscriber for Selected MNOs³⁵

2. Handset Manufacturer Trends

Given the impending market saturation, handset manufacturers will compete more and more aggressively for lower numbers of new consumers. For the near term, smartphones will be less affected by this situation because that market is still growing. Figure 13 illustrates the percent breakdown of the handset market between smartphones and feature phones. The number of smartphones in the market is predicted to overtake the number of feature phones by the end of 2011 (MarketsandMarkets, 2010). As smartphones reach the saturation point in adopters, competition between handset manufacturers will intensify.

³⁵ After FCC (2010b). EBITDA is a measure of profitability based on accounting profits before deducting interest expenses, corporate income taxes, depreciation, and amortization.

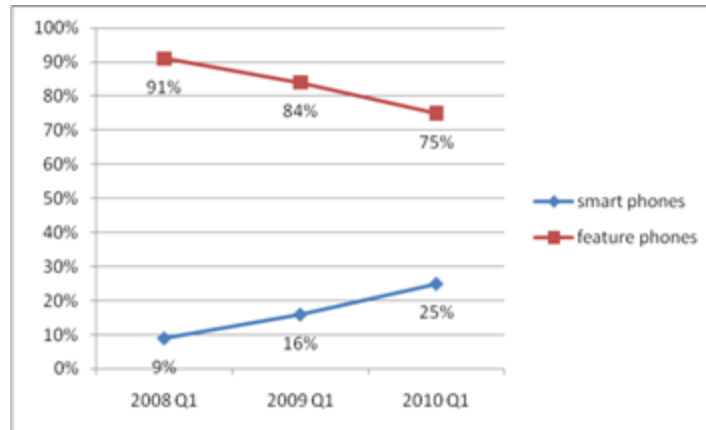


Figure 13. Handset Market Share of Smartphones and Feature Phones³⁶

New entrants into the smartphone market will also contribute to increases in rivalry.³⁷ This increased rivalry will be fueled by the convergence of smartphone capabilities with those of PCs; and, like the PC, smartphones will likely begin to become commoditized. Less expensive components will decrease handset costs as well as barriers to entry for both handset manufacturers and their hardware suppliers. Figure 14 illustrates the reduction in smartphone selling price between 2006 and 2009. This scenario will result in an overall weakening of the bargaining power those firms in the handset market.

³⁶ From MarketsandMarkets (2010).

³⁷ Between 2006 and 2009, the number of handset manufacturers that distribute within the United States increased from eight to 16 (FCC, 2010b).

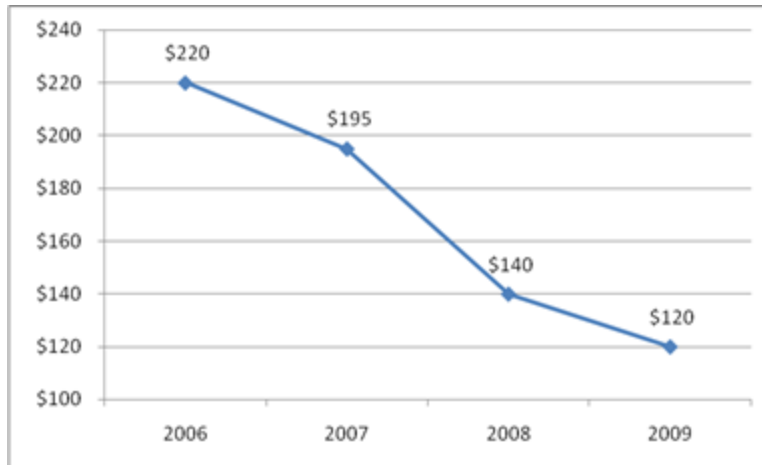


Figure 14. Average Smartphone Selling Price³⁸

The weakening of handset manufacturer bargaining power gives OS providers an opportunity to potentially gain greater value from the handset market. Among suppliers, OS providers maintain a unique position among handset component providers. For example, people commonly use the term *Android Phone* to describe smartphones running the Android OS. This circumstance provides them with a great deal of leverage in the form of marketing potential. Given a small field of OS providers and the commoditization of handsets, a situation similar to what occurred between Microsoft and PC-makers in the 1990s could reoccur. At that time, Microsoft, enjoying a near monopoly as an OS provider to PC-makers, raised the price of its OS and caused an erosion of profitability throughout the PC market (Porter, 2008). Handset manufacturers who do not vertically integrate (provide their own OS) risk suffering a similar fate. The potential for this scenario to occur will likely induce smartphone manufacturers to pursue partnerships with OS providers or work to gain a competency in developing their own value-added OS.

Vertically integrated smartphone manufacturers, such as Apple and RIM, are better positioned. Like the Macintosh computer, the Apple iPhone will continue to differentiate itself from the commodity handsets, potentially creating a separate market space and avoiding commoditization. RIM has the same opportunity, and it will likely

³⁸ After FCC (2010b). Dollar values represent smart phone prices after provider subsidies. MarketsandMarkets presents similar data showing the same trend in prices before subsidies.

maintain a decent hold on the corporate market due to its focus on integrated security features. The performance of competing security solutions will depend on consumers' perceptions of the price-performance tradeoffs.

3. Security in the Mobile Communications Industry

Commercial market trends in the inclusion of security functionality influence the extent to which the DoD requires a separate architecture to facilitate secure mobile communications. The current DoD solution, the secure mobile encrypted portable electronic device (SME PED), uses commercial services provided by MNOs (including RANs, core networks, and services) for mobility. The SME PED leverages handset controls with limited government-operated infrastructure controls to protect data (e.g., antitamper design, end-to-end cryptography, and hardware separation).³⁹ This demonstrated solution shows that, at most, the DoD does not require a separate infrastructure if it utilizes a handset capable of sufficiently protecting information residing on, and transiting between, network end points (e.g., handsets, servers, and databases). The SME PED exists because the DoD has historically been unable to obtain commercially provided solutions. However, reduced bargaining power of handset manufacturers and increased visibility of security functionality indicates that the potential exists for successfully acquiring suitable solutions at market prices. RIM's smartphone market share indicates that an appreciable number of corporations value security, but the iPhone's reported growth in the corporate segment highlights the struggle between demand for security and demand for greater functionality in the commercial industry.⁴⁰

a. The Meaning of the Term "Security"

The terms secure and security can take on widely varying meanings, depending on subject matter and context. In this work, the terms security and secure refer to the concepts presented by the National Institute of Standards and Technology (NIST) in its widely accepted definition of computer security. This definition exists in terms of

³⁹ See Appendix E for a brief list of features.

⁴⁰ Report on iPhone's growth in the enterprise market: "iPhone Infiltrates Corporate World with Help of Security Apps." Source: Channel Insider (2011). Pages 1-3. Retrieved from EBSCOhost database.

the confidentiality, integrity, and availability of information systems and the data stored therein. The NIST Special Publication 800-12 (1995) has stated that these principles also apply to network security. The following list summarizes the definition:⁴¹

- Computer Security—Extending protection to an information system in order to preserve the confidentiality, integrity, and availability of system resources. These resources include hardware, software, data, and telecommunications (i.e., data in transit).
 - Confidentiality—The requirement to safeguard private information from disclosure to unauthorized entities.
 - Integrity—Integrity includes timeliness, accuracy, completeness, and consistency of information. However, as computers cannot guarantee all of these qualities, integrity is separated into the following two categories: Integrity includes maintaining information nonrepudiation and authenticity.
 - Data integrity—“A requirement that information and programs are changed only in a specified and authorized manner” (as cited in NIST, 1995).
 - System integrity—A requirement that a system “performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system” (as cited in NIST, 1995).
 - Authenticity—The property of genuineness and the ability to be verified and trusted, resulting in confidence that a transmission, message, or message originator is valid.
 - Nonrepudiation—False denial of having executed a particular action or instruction.
 - Availability—Timely and reliable access to, and use of, information.

⁴¹ Definitions from NIST Special Publications 800-12 (1995) and 800-53 (2010). Available from <http://www.nist.gov/publication-portal.cfm>.

b. The Supply of Security in the Commercial Market

Sabat (2003) has argued that scale and scope economies drive emerging market trends,⁴² alluding to the notion that custom solutions are more expensive because of their limited economies of scale. Based on Sabat's assertions, a solution meeting the needs of more buyer groups will proliferate more quickly at the most economical prices for all buyers.

Some commercial security solutions claim to rely on a multiple independent levels of security (MILS) architecture,⁴³ defined as a high assurance architecture designed to enable secure information partitioning (Boettcher, Delong, Rushby, & Sifre, 2008). Other, possibly more effective, high assurance security architectures exist.⁴⁴ A commercial high assurance separation, or similar, architecture may potentially be used to implement the following government concepts:

- Cross domain solutions (CDS)—“controlled interface [devices] that provide the ability to manually and/or automatically access and/or transfer information between different security domains” (Committee on National Security Systems, 2010).
- Multilevel secure (MLS) systems that enforce national policy with respect to the protection of information.⁴⁵

The Committee on National Security Systems (CNSS, 2010), defines MLS as the “concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization” (p. 47). It defines MSL as a “capability of an

⁴² Scale refers to the property of decreasing total cost as output increases (Mankiw 2006). Scope involves reaching broader market segments as implied by Sabat's argument that applications development platforms drive scope economies.

⁴³ For example, see SYSGO's discussion of its PikeOS security certification at <http://www.sysgo.com/products/pikeos-rtos-and-virtualization/security-certification/>.

⁴⁴ See Levin, Irvine, and Nguyen (2006), for example.

⁴⁵ Refer to Office of the Director of National Intelligence (ODNI, 2007).

information system that is trusted to contain, and maintain separation between, resources (particularly stored data) of different security domains” (CNSS, 2010, p. 48).⁴⁶

Currently, RIM’s BlackBerry represents the foremost provider of security to the commercial market (Reed, 2010). RIM markets an enterprise solution to government and corporate customers providing encryption, strong authentication, and remote device administration (RIM, 2011). Their integrated architecture and services provide a much higher degree of confidentiality, integrity, and availability than standalone handsets. This fact, combined with RIM’s strong brand image for providing enterprise services and the smartphone’s strength in meeting corporate users’ needs,⁴⁷ helps explain RIM’s early and continued dominance of the enterprise smartphone market. Still, the comparison of selected security features in Table 4 shows that the BlackBerry Enterprise solution does not provide security services comparable to SME PED devices.

	SME PED	BlackBerry
High assurance separation architecture	✓	
Domain switching	✓	
CAC reader	✓	✓
Type 1 encryption capability	✓	
Non Type 1 encryption capability	✓	✓
SCIP** capability*	✓	
HAIPE capability*	✓	
GSM network compatibility	✓	✓
CDMA network compatibility	✓	✓
Wi-fi network compatibility	Some devices	Some devices
Data sensitivity certification	At least Secret	Sensitive but unclassified
*Enables secure voice or data communications		
**Secure Communications Interoperability Protocol		

Table 4. Comparison of Selected Security Features in BlackBerry and SME PED Devices⁴⁸

⁴⁶ These definitions are cited in NIST’s *Glossary of Key Information Security Terms*. Available from [http://www.nist.gov]. MLS is defined similarly by the IETF (2000).

⁴⁷ RIM was ranked number 63 on Interbrand’s top 100 best global brands in 2009, and it received the Best Mobile Enterprise Product or Service award from the GSMA (Datamonitor, 2010a).

⁴⁸ After: GD Sectera Edge Literature (n.d.), available from [http://www.gdc4s.com/]; L-3 Guardian Data Sheet (2007), available from [http://www.l-3com.com]; http://us.blackberry.com/ataglance/security.

Virtualization represents a key feature that enables the replication of OS functionality in multiple domains. Commercial adoption of virtual machine support on handsets, combined with MLS policy enforcement, would represent a major step toward potentially achieving overlap between commercial and DoD security requirements. Use of virtualization to separate resources between domains appears to be the implementation that has gained traction among both hardware and software companies. Table 5 provides examples of firms that are currently working, or have recently worked, to implement solutions that employ virtualization on mobile platforms to separate domains. This table includes firms that are producing both Type 1 and Type 2 virtual machine monitors (VMM). Type 1 pertains to implementations on hardware, while Type 2 refers to software implementations within a host operating system.⁴⁹ Chapter III provides more technical discussion on this subject.

Firm	Major Partner
VMWare	LG
Xen	Samsung
Open Kernel Labs	Motorola, ST-Ericsson
Red Bend (VirtualLogix)	Multiple
SYSGO	Multiple
Wind River	Samsung

Table 5. Examples of Multilevel Handset Efforts⁵⁰

One website includes the following in its short list of requirements for such technology to gain popularity: the need for a mobile device powerful enough to support virtualization while maintaining a level of usability commensurate with other devices on the market (Virtualization.info, 2008). This statement suggests that the relatively low level of processing power in handsets has been a contributing factor to the

⁴⁹ Brodtkin (2010) refers.

⁵⁰ From multiple sources: Luna (2010); Red Bend Software (2011); Virtualization.info (2008); Suh (2007); Nunez (2010); <http://www.ok-labs.com/solutions/the-okl4-microkernel-advantage>; <http://www.sysgo.com>; <http://www.windriver.com/>.

absence of strong security features. Although the impetus to virtualize has centered on improved functionality and efficiency, these firms and their partners have displayed a willingness to market the security benefits of their solutions.

The security technology company Koolspan provides a solution called Trustchip that acts as an interface between the handset and the network to create an encrypted tunnel and protect data in transit (J. McGann, personal communication, 10 February 2011). The Trustchip is part of a larger solution that facilitates management of symmetric keys and allows remote administration. Koolspan promotes its solution to corporations such as law firms, financial intermediaries, and international corporations (McGann, personal communication, 10 February 2011). Furthermore, Koolspan partnered with AT&T in the past to provide an encrypted voice communications capability to enterprise, government, and law enforcement customers.

These examples do not, of themselves, indicate the existence of a high assurance secure mobile communications market, but they do show that efforts exist to provide competitive commercial security solutions. This situation is important because, whereas leaders like RIM may prefer to maintain their virtual monopoly instead of developing solutions for the DoD, new firms that are trying to establish themselves may be much more willing to work and innovate in the provision of security features. The multiple existing partnerships also indicate the willingness of other market participants to invest in the development of security-enhancing features.

In accordance with the economic definition of a market,⁵¹ the existence of a commercial market for secure communications requires both supply of security technology and demand for security features. However, a discrete gap exists between commercial and DoD demand for security functionality.

⁵¹ Mankiw (2006) defines a market as “a group of buyers and sellers of a particular good or service,” 64.

c. Potential Sources of the Gap Between DoD and Commercial Demand for Security

The DoD has historically taken a very conservative approach to protecting information due to the high impact of a compromise of classified information. A 1970 report by Ware (1970) demonstrates the organization's longstanding perception of high risk. The relatively low commercial demand for security features provides little incentive for producers to develop secure communications capabilities that meet both DoD and commercial requirements.

The magnitude of commercial demand depends on buyers' perceptions of the value added by security technology. Buyers' perceived values dictate their actions (Peppard & Rylander, 2002); therefore, they will demand security commensurate with their perception of the value of (or risk to) the confidentiality, integrity, and availability of their information. This argument leads to the conclusion that residential consumers will demand (and be willing to pay for) increased security functionality as they use mobile devices for more sensitive transactions (e.g., mobile commerce activities).

The fact that most people do not judge probability well (Wildavsky & Wildavsky, 2008) can result in incorrect evaluation of risk. This situation offers an explanation of the lag in demand for security versus functionality. Use of a formalized risk management process can help mitigate this situation, but the technical complexities of the computer and telecommunications environment can lead even subject matter experts to underestimate their risk exposure. As an example, Luallen and Hamburg (2010) reported that 24% of industrial control systems professionals indicated a disbelief in threats that could affect their operations.

Corporations who employ a formal risk assessment process, such as that described by NIST (2002), should achieve more accurate risk assessments; however, regulations meant to ensure the persistence of information security or privacy may inadvertently interfere with the risk assessment process. For instance, medical organizations tend to prioritize HIPAA requirements over protecting information.⁵² They

⁵² Based on the experience of the privacy company, WebLOQ (G. Sidman, personal communication, 18 November 2010).

aim first to reach regulatory compliance, and after doing so, they may never reach beyond that threshold. The regulation potentially creates a ceiling for security efforts instead of enhancing security posture. In this situation, corporations' focus on increased security is replaced with a focus on satisfying the regulatory requirements—i.e., the perceived risk of not following the regulation outweighs the perceived risk of not providing robust security controls.

4. Potential Ways Forward

Based on the above Five Forces analysis and analysis of trends affecting the MNO and handset markets, this subsection discusses potential areas in which the DoD can work with market participants to achieve lower cost equipment, lower cost services, increased network and handset functionality, and maintain or improve the overall level of security.

It is in the handset that the DoD's requirements for high assurance security features differ most from those of residential and corporate customers. The potential cost of meeting these requirements depends on a number of factors, and is therefore highly variable. Many of these factors depend on the amount of perceived value that both producers and consumers hold for security-enhancing features.

During this early stage, the DoD has the opportunity to influence the outcome of the “winning” solution, if one exists that can serve both commercial and government needs. Broad industry acceptance of Suite B⁵³ would represent a successful example. If security providers believe that its inclusion in all products will enhance profits, then they are more likely to work toward its implementation. Ultimately, the expectation of obtaining greater profits depends on consumers' perceptions that “government-grade” encryption, in this case, adds value to the product.

Each of the DoD's strategic options, discussed in the following subsections, may require gaining or augmenting its organizational competencies in order to execute that strategy.

⁵³ Suite B is a set of cryptographic algorithms for protecting information up to the Secret level. See http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml.

a. Leverage MVNO Flexibility

In regard to network operators, changes in the market may allow the DoD to reap savings while obtaining equivalent or better service than it is currently obtaining. Market saturation may induce MNOs to seek additional revenues from resellers and MVNOs, thereby making it easier for new entrants to start MVNO operations. This is especially true if the MVNE and MVNA markets expand, prompting those firms to offer expanded services and support while competing on quality. Given the trends in the MNO market, the opportunity for the DoD to implement an MVNO business model could increase.

The DoD may employ an MVNE or MVNA to facilitate acting as an MVNO (i.e., incur costs and provide services to DoD personnel in the same way that an MVNO provides service to consumers). Alternatively, the DoD may utilize the services of an existing MVNO that can tailor its business to the DoD's particular values. The DoD's current model requires purchasing wireless services in the same way as residential consumers. The advantage of acting as an MVNO is that prices of network-based services (voice minutes and data amounts) will be wholesale prices, which, at greater volumes, potentially bring greater savings. Chapter IV provides further analysis of this approach.

DoD's application of the MVNO business case does not imply competition with commercial MNOs, but this scenario represents a potential unintended consequence if the industry perceives DoD's actions as threatening to their business. As such, implementation of this strategy would require careful management of signals and monitoring of industry perceptions.

Additionally, acting as an MVNO would provide the flexibility to purchase handsets directly from manufacturers instead of through intermediaries—the current practice. These purchases would occur at wholesale rates, and this strategy would afford the DoD more flexibility in obtaining commercial handsets that best suit its needs. The drawback to this strategy is that it requires developing a competency regarding handset acquisition.

b. Exploit Handset Manufacturers' Reduced Bargaining Power

In the handset market, reduction of handset manufacturers' ability to differentiate will reduce their bargaining power, thus increasing buyers' opportunities to obtain higher quality handsets at potentially lower costs. The increasing competition among handset manufacturers may facilitate buyers' attainment of new features (e.g., security functionality) due to increased negotiating leverage for buyers. Ultimately, the outcome of a negotiation will depend on a multitude of quantifiable and nonquantifiable factors. In theory, a firm will decide to undertake a venture if the net present value (NPV) of that investment is projected to be positive—in other words, if the expected benefit outweighs the estimated cost; however, in reality, future expectations are subject to manipulation or miscalculation due to a multitude of potential factors including the subjective nature of prediction. For example, after Hewlett Packard's (HP) acquisition of Palm in 2010, the head of HP's Personal Systems Group made the following statements (Edwards, 2010): "Some analysts were saying Palm was worth nothing. And some people said it was worth \$14 a share. We paid \$5.70 a share. We judged our willingness to pay based on the opportunity." These words exemplify the fact that a firm's willingness to undertake new ventures depends on its assessment of the opportunity at the time. For all handset manufacturers, the strong drive for firms to maximize economies of scale and scope⁵⁴ provides potential leverage for influencing them to undertake new types of ventures as the market approaches saturation.

c. Team With Large Corporations

The overlap between government and corporate requirements that are different from those of residential users would foster a niche subindustry. The demand for unique capabilities may limit the providers, thereby increasing rivalry while also increasing buyer power due to the relatively small number of buyers who purchase large

⁵⁴ Sabat (2003) has argued that scale and scope economies are the major driving forces of growth in the mobile wireless industry.

quantities. Security functionality is one potential area where sufficient overlap of requirements exists, especially for those major corporations with a need for high assurance data protection.

d. Education

To date, a gap has existed between commercial and DoD demands for security functionality. This gap may be partially driven by misperceptions of risk. Assuming that users will perceive greater personal risk as they engage in transactions involving more sensitive information, such as banking activities via mobile devices, this gap should lessen with time. However, a strategy to increase awareness and understanding may contribute toward reducing the gap more quickly. For instance, the DoD may benefit from participation in a joint education campaign with academia and industry participants to improve the accuracy of consumers' perceptions of vulnerabilities and threats. Such a strategy might also be effective when implemented on the supply side—for standards developers, manufacturers, and service providers. Such an effort may yield improved awareness of security issues, more robust development practices, and ultimately lead to improved security functionality in COTS software.⁵⁵

⁵⁵ This conclusion is supported by Davidson. See <http://blogs.oracle.com/maryannndavidson>.

III. BUSINESS CASE ANALYSIS FOR SECURE COTS HANDSETS

This chapter outlines a business case for leveraging COTS technology to reduce the traditional high cost of secure mobile technology (e.g., SME PED), increase functionality, and maintain or improve the level of security.⁵⁶ However, to provide the same high level of security found in currently fielded devices and increase functionality, some tradeoffs are required. This chapter will discuss the tradeoffs and costs associated with the estimated reduction in risk. Figure 15 provides an illustration of the desired characteristics for the business case. This chapter highlights a business case that potentially meets all three characteristics. The ideal system provides high levels of security and functionality at a low cost. In contrast, the SME PEDs provide high levels of security and functionality (i.e., the devices meet the thresholds of the smartphone definition provided in Chapter II); however, given the current level of demand in the DoD, the devices are extremely costly from a Total Cost of Ownership (TCO) perspective.

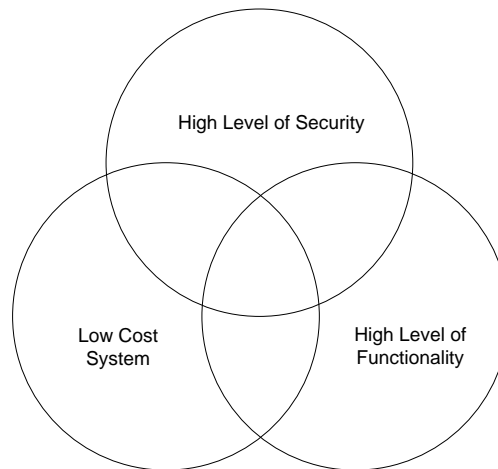


Figure 15. Desired Characteristics

⁵⁶ Refer to Chapter II for a discussion of security.

A. BASELINE ASSUMPTIONS

Based on the mobile industry analysis presented in Chapter II, the authors assume the current method for procuring secure mobile communications is not optimal. The industry is continually evolving and producing innovative technology outside of the smaller military niche market. For example, according to their product sheets, the SME PEDs—developed for a government-only market—seem behind the commercial market in the availability of innovative features (e.g., until recently the devices lacked the ability to connect to wireless local access networks).

1. Total Cost of Ownership

When considering the TCO for secure smartphone communications, the cost of service is included with the device cost. In the commercial market, the network operators subsidize the handsets to increase their average revenue per user (ARPU), which ultimately increases the consumer's TCO (i.e., device cost + service cost across the duration of the plan + switching cost) (Global Industry Analysts, 2010). Essentially, subscribers are offered a lower initial cost for their phone if they agree to a longer service contract—in the end, the network operators increase their ARPU. As described in Chapter II, the authors assume that this type of transaction is mutually beneficial or it would not continue to occur.

In Figure 16, the first (topmost) option illustrates a two-year service contract with a subsidized smartphone device (i.e., network provider pays a proportion of the handset cost). The second option illustrates the nonsubsidized device with a change in providers during year two for the lower-priced plan. The third option also illustrates a subsidized device, but the customer decides to end the contract halfway through execution and switch providers. In so doing, he incurs switching costs (i.e., the cost to cancel the original contract). The TCO for options 1 and 3 are \$2070 and \$2130, respectively, but the TCO for the option 2 device is only \$1980. The takeaway from this example is the device TCO should consider the duration of the service plan when negotiating the procurement. Using the SME PEDs as an example, the current process requires customers to choose the carrier prior to procuring the device (i.e., the device's air interface chip

needs to match carrier's signal). Once the device is procured, the customers are locked into the carrier until they change hardware. As previously mentioned, the handset hardware is extremely expensive, making the option to change carriers cost prohibitive (i.e., the high cost hardware reduces flexibility for the customer).

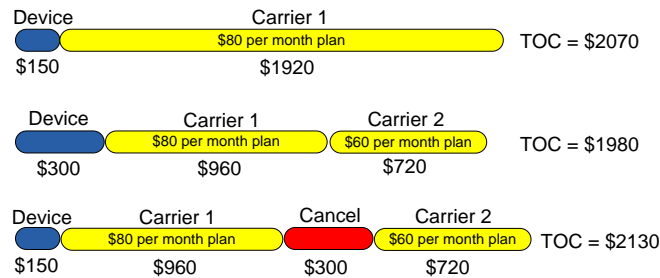


Figure 16. Total Cost of Ownership Options

2. Base Case Platform (SME PED)

Based on the current U.S. government secure smartphone products (i.e., the General Dynamics [GD] Sectera and the L-3 Communications [L3] Guardian), this paper assumes that the current costs are too significant for defense-wide adoption—as evidenced by fewer than ten thousand handset purchases over the past half-decade.⁵⁷ According to the National Security Agency (NSA) program office (I851), the Sectera product was developed as a partnership between NSA and GD. The Guardian device was independently developed, certified, and accredited under an L3 research and development (R&D) program. The original R&D contract was awarded as a shared effort where the government shared the R&D cost with the contractors—the initial R&D cost to the government for both devices is about \$38M.⁵⁸ Later, the government distributed an additional \$5.5M to GD for upgrades to include forced reauthentication, black-side antivirus, DISN security accreditation working group accreditation, Secure Communication Interoperability Protocol-232 North Atlantic Treaty Organization cryptographic mode, top secret data, red side antivirus, and e-mail classification.

⁵⁷ This fact is discussed later in the chapter.

⁵⁸ In addition to \$4M of R&D cost for the network architecture.

According to the program office, the high unit price is representative of low volume procurements and routinely evolving requirements. The device's cost totals about \$4,000 to procure the handsets, antivirus client software, and additional hardware accessories. Other costs that a customer can expect to incur include: approximately \$1,000 for the connecting local server, longer than commercial lead times resulting from bundled procurements, and an ultimately reduced feature set relative to commercial devices. The reduction in features stems from low volume orders that do not justify frequent technology refreshes. Additionally, the supply duopoly has strong potential for limiting future innovations due to the absence of competition. For example, a government-only product without a requirement for additional capabilities provides a disincentive for suppliers to incorporate future technology advances (i.e., a lack in demand leads to a lack in supply). However, since the devices remotely access classified networks (i.e., the Defense Information System Network [DISN]) the authors assume the device properties are adequate for processing this level of information; therefore, this chapter will focus on highlighting less costly alternatives that have potential to provide at least the same level of assurances regarding computer security defined in Chapter II. Refer to Appendix F for a summary of the SME PED features.

According to the same program office, and consistent with trends in recent delivery orders, the SME PED annual demand is estimated at 1,500–2,000 devices. As of February 2010, the total quantity procured since the program's inception is about 5,500 devices.⁵⁹ Given this demand and an average \$4,000 per device, the annual amortized (i.e., across two-year estimated lifetime) expenditures for SME PED devices are calculated at \$4M per year—this cost only includes the cost of handset equipment and accessories. The wide area network (WAN) service for these devices is provided over the commercial networks and, therefore, the handset TCO should include the wireless connection cost. According to the program office, in addition to the monthly reoccurring service charge there is an annual reoccurring fixed cost, independent of demand, for connecting the SME PEDs to the Defense Information Systems Agency's (DISAs) networks (i.e., the DISN)—approximately \$2M per year.

⁵⁹ I851 Program office provided total.

As discussed earlier, when evaluating the TCO for mobile handsets the cost of services is included in the calculation; however, for this chapter the cost of service is excluded. Chapter IV more thoroughly details the associated service cost. These procurement trends only represent the SME PED demand. The DoD currently has a significant demand for secure fixed or wireline devices (e.g., Secure Terminal Equipment [STE]) and basic mobile phone devices (e.g., Qualcomm QSec). These trends were not included in the analysis, because this research focused on requirements akin to those of a smartphone. This paper assumes that, if the cost to procure secure smartphone capabilities is significantly reduced, the candidate devices might replace the traditional STE or QSec requirements.

An area of interest when considering cost is the cost of the next feature based on the current SME PED model. Figure 17 illustrates the various feature upgrades to the Sectera Edge device on the horizontal axis and their associated cost to the government on the vertical.⁶⁰ The figure includes DSAWG (Defense Information Assurance Security Accreditation Working Group) accreditation because it represents a significant cost for system changes affecting information assurance. Based on these historical costs, the average cost for an upgrade is \$790K with a standard deviation of \$250K and a confidence level (95%) of 0.61. The low scoring confidence level (i.e., high variability between upgrades) leads to the conclusion that, within a rough order of magnitude, a future feature might cost the government between hundreds of thousands and a few million dollars.

⁶⁰ NSA (i851) provided data.

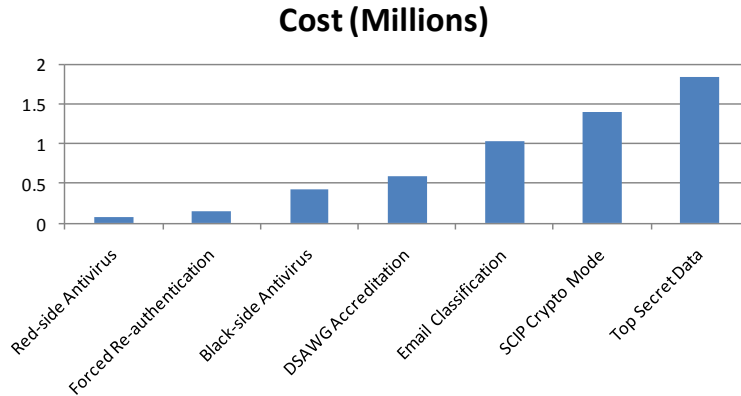


Figure 17. Sectera Edge Upgrade Cost (Millions)

3. Proposed Platform (Commercial Device)

Since the SME PED devices provide the functionality to securely communicate independently within two separate sensitivity domains, this paper assumes the ideal COTS solution must provide a similar multi-domain capability. In order to prevent information from spilling across domains, DoD (i.e., Unified Cross Domain Management Office [UCDMO]) policy requires additional assurances to mitigate risk.⁶¹ In an effort to maintain the high functionality commonly provided by modern day high-end operating systems and to reduce the amount of components, potentially suitable COTS security architectures may virtualize (i.e., through a Virtual Machine Monitor [VMM]) the guest OS for each domain while using a high assurance VMM as the underlying separation platform. As discussed in the previous chapter, the commercial market is moving toward the provision of such architectures on handsets. However, none of the previously mentioned operating systems is listed as an UCDMO-approved solution.⁶² This is important to note when considering acquisition procurements, but not a significant deterrent when considering technology feasibility.

In the architectural approach described above, a lower layer separation kernel provides the device's high assurance security functionality. Many separation kernels exist

⁶¹ Refer to CJCSI 6211.02B, Defense Information System Network and Connected Systems, 31 July 2003 for further details.

⁶² Reference UCDMO Baseline Version 3.7.0.

and differ drastically in implementation, but they share the same basic property of providing isolation or resource partitioning to prevent sharing and limit covert channels (Levin, Irvine, & Nguyen, 2006). Essentially, when resources are shared across domains, the addition of nonkernel trusted elements to the architecture increases its potential for malicious activity or unintentional starvation. For example, given two independent processes on two independent processors, the probability of information transferring from one process to the other is very low. However, when the processes share resources, including the processor, the probability of policy violation increases with information transfer. Care must be taken to identify all possible overt and covert information flow channels (Lampson, 1973). Another important characteristic absent from commercial offerings of separation kernels is the concept of least privilege, which can assist in limiting users or programs from exceeding their authority. This not only protects the system from unintentional accidents or errors, but also additionally assists in mitigating potential malicious activity (Levin, Irvine, & Nguyen, 2006). As mentioned before, the commercial market provides various CDSs for high-end computing systems; however, no smartphone solution is available with a Common Criteria Evaluated Assurance Level (EAL) 6+ certification.⁶³ The business case for leveraging this concept on smartphone devices has traditionally failed to exist because of a lack of resources required to host multiple domains. However, given recent innovations, the resources (i.e., ARM Cortex A9 or A15) needed to support a CDS capability may now exist. In a phone discussion, one manufacturer mentioned staffing this idea in the past; however, the firm determined that the cost was not commensurate with the potential benefit.

Figure 18 illustrates an abstract example of a separation architecture. The VMM in this figure virtualizes the different untrusted subjects—guest operating systems (e.g., android, iOS, Windows Mobile, etc.). For a more in-depth technical discussion on the advantages and disadvantages of the various solutions, refer to the UCDMO.

⁶³ Appendix A provides an introductory discussion of the Common Criteria.

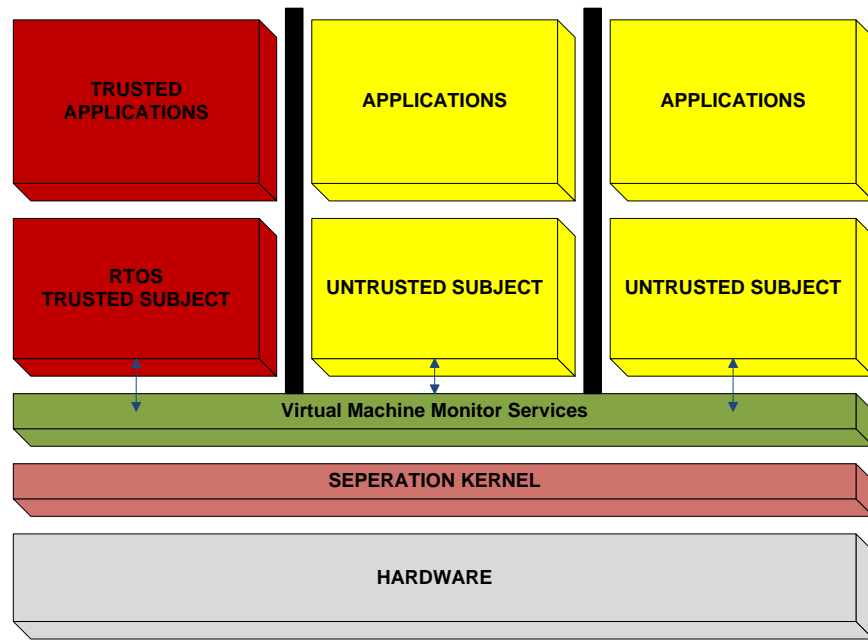


Figure 18. Cross Domain Solution Example⁶⁴

B. COST

1. CDS Architecture Cost

Since a COTS smartphone containing a high assurance separation kernel acting as a VMM is not currently available in a competitive open market, the value for this technology is still difficult to discern. Therefore, the authors assume that the value of such an architecture lies between the manufacturer's willingness to pay and the platform (software) provider's willingness to accept. The next two subsections provide different perspectives (i.e., manufacturer, and platform provider) on the value of a high assurance separation architecture implanted on a smartphone device.

a. Manufacturer Perspective (Willingness to Buy)

Based on conversations with handset manufacturers, the aggregated willingness to pay for an architecture intended to meet high assurance separation objectives on modern smartphone devices, described above, is listed in Table 6. The

⁶⁴ Image generated from (Uchenick, et al., 2005), (Boettcher, et al., 2008) and the description found in (Levin, et al., 2006).

manufacturer licensing fee is the price the platform provider charges to license the software per device. These cost estimates assume the manufacturer has enough bargaining power to control the prices for the CDS platform providers.

MILS Software Through Manufacturer	Low	High
manufacturer licensing fee	\$ 1,500,000.00	\$ 5,000,000.00
Development License (SDK)	\$ 50,000.00	\$ 100,000.00
Per developer license	\$ 1,000,000.00	\$ 2,000,000.00
Total	\$ 2,550,000.00	\$ 7,100,000.00

Table 6. Manufacturer Option

According to a leading manufacturer, these estimates seem reasonable because these platform providers are not current players in the handset market.⁶⁵ The manufacturer-driven solution would provide the platform providers an entry into the handset market. In Table 6, the manufacturer licensing fees are estimated at \$0.10 to \$1.50 per phone with a 10–50M device volume.⁶⁶ The manufacturer might incur some upfront development costs, but these costs are highly variable based on the strength of the negotiations. The software development kit (SDK) and developer license cost seem fairly consistent across multiple providers—these estimates assume enterprise pricing for developers. Those SDK and individual developer license costs are potential necessities if the receiving organization requires the trusted subject or microkernel to run trusted applications for evolving mission critical functions vice a guest OS using inherently untrusted programs. The burdens of the developer licensing fees are endured by the organizations willing to build trusted applications.

b. Platform Provider Perspective (Willingness to Sell)

If the DoD were to develop and advance the technology using its own funding, the potential range of costs could exceed those of the manufacturer. Table 7 illustrates costs the DoD could expect to pay for the technology—these costs are slightly

⁶⁵ January 2011 discussion.

⁶⁶ These numbers represent manufacturer’s willingness to pay. The actual price will greatly depend on each organization’s negotiation strengths.

higher than the manufacturers' option.⁶⁷ These estimates only represent a few platform providers' perspectives. The actual cost could drastically differ depending on deviations from their current roadmaps, the complexity contained within the various layers, the design of the architecture, etc. Due to potential unknown high assurance development considerations, the maximum cost for the technology could exceed the estimates presented in Table 7.

MILS Software Through DoD Acquisitions	Low	High
Porting code to prototype	\$ 100,000.00	\$ 1,000,000.00
runtime license	\$ 2,000,000.00	\$ 6,000,000.00
Development License (SDK)	\$ 50,000.00	\$ 100,000.00
Per developer license	\$ 1,000,000.00	\$ 2,000,000.00
Total	\$ 3,150,000.00	\$ 9,100,000.00

Table 7. DoD Acquisition Process Option

This seems reasonable since the DoD has very little buying power when compared to the commercial market, which provides greater volume. The costs in Table 7 were aggregates of platform providers' estimates. The cost varies depending on the intended platform. For example, some providers' software is embedded on the chip, requiring specific processor compatibility. If the provider's product line was built around different technology than the desired platform (e.g., platform provider's software was built on an Intel processor and the requested handset leveraged an ARM processor), the necessary porting would require a significant amount of reengineering. The estimated porting prices for these products were about double the price in Table 7.

Considering the cost to the DoD, the two development approaches (i.e., commercial manufacturer vs. platform provider) would drastically differ. The authors assume the commercial manufacturer would incur the burden of the software license fees during sales as a percentage of revenue. The DoD procurement option would incur the burden of licensing fees during the R&D phase. From the CDS platform provider perspective, it seems less risky to opt for the intrinsic value (i.e., the DoD option); however, the option value seems more valuable considering the return. The real option

⁶⁷ These price points were aggregated from a couple different platform providers.

value could provide an entry into the market, product line architecture monopoly, and additional unintended innovations that the consumer adapts into a disruptive technology. Since the price per unit drastically depends on procurement negotiations and volume, it is difficult to enumerate price based on known costs. Given that RIM is the current commercial North American smartphone market leader and provides a valued security solution, it seems feasible that the high assurance secure architecture implemented on COTS phones would proliferate as a threatening competitor. If this becomes reality, then the cost for this technology will likely be representative of today's current RIM device (i.e., leveraging economies of scales).

2. Encryption Cost

Once these devices support a high assurance secure architecture, the next valued capability is noncryptographic controlled item (CCI) encryption algorithms. The current SME PED devices leverage the NSA-certified Type 1 encryptor (e.g., High Assurance Internet Protocol Encryptor [HAIPE]).⁶⁸ This paper considers the dedicated hardware required to support the Type 1 encryption capability as an added cost. If the device hosts HAIPE hardware—requiring a classification of CCI—the handheld device becomes less mobile and constrained in marketability. Mobility is reduced since DoD policy requires added physical security measures (e.g., DoD policy requires that CCI equipment remain in constant possession or secured in an approved location). Additionally, the market size is constrained, because the CCI classification requires export controls. Alternatively, to assist in reducing cost by increasing the potential market the CDS approach could leverage a non-CCI HAIPE (e.g., Suite B, Cryptographic High Value Product (CHVP)) (National Security Agency, 2010). The cost to procure a HAIPE Suite B capability is difficult to estimate since the commercial market does not offer an approved NSA-certified and accredited smartphone client. Considering that the commercial market provides various noncertified solutions, the cost for this capability takes on a broad range

⁶⁸ Sourced from the website: http://www.disa.mil/services/SME_PED.html.

depending on requirements. According to various vendors, if the manufacturers adopt this technology, the cost to develop and produce the encryption functionality is currently projected at less than a few dollars per device.⁶⁹

3. Future Features Upgrades

Based on the earlier SME PED discussion regarding the associated cost of adding features, this section assumes the commercial market manufacturer cost is similar to what the government spent for the SME PED upgrades.⁷⁰ The current SME PED demand yields an estimate of the cost for each aftermarket feature to equal about \$260 per device. This assumption is based on the average cost for each additional feature. As highlighted in the beginning of this chapter, the average cost per SME PED feature is about \$790K. If the DoD leverages the commercial market economies of scale (i.e., 10 to 50M devices), each upgraded feature would result in a cost of \$0.02–\$0.79 per device. These high volume markets provide lower cost, but traditionally require a more feature-rich device. Assuming that an architecture exists which meets high assurance security requirements while also providing the features expected of other smartphone OSs, the market may adopt a more secure solution—especially since the banking and medical industries have a strong financial interest in protecting their information.

4. Additional Costs

Additional costs not included in this analysis are commercial application development for DoD-specific requirements, reduced procurement lead times, maintenance and support, internally developed applications, and technology refresh every 2–3 years. Some of these costs appear negligible since these devices are potentially becoming commoditized. For example, as mentioned in the industry analysis section, the convergence of multiple 3G chipsets (e.g., CDMA2000, WCDMA, UMTS, etc.) into a single 4G technology (i.e., LTE) creates the potential for larger volumes in the converged market. Since three of the four major carriers invested in the LTE technology, their future

⁶⁹ Some vendors that provide this functionality are: certicom, cellcrypt, koolspan, fortress technologies, etc.

⁷⁰ Reference Chapter III, Section A, Paragraph 2.

smartphones could potentially share the same chipset. This could create a larger market for the chipset manufacturers and contribute toward commoditizing the component. However, since the FCC is auctioning the LTE spectrum across fragmented frequency bands, this single chipset concept might fail to materialize.

C. BENEFITS

The benefits received from leveraging CDS smartphones vary drastically across the quantifiable space. For example, assuming the CDS smartphone contains enough resources and implements the correct security properties to run more than two domains, this could facilitate accessing the DISN while on the move. The ability to access multiple domains (i.e., Internet/NIPR/SIPR/JWICS) from one device without requiring a stationary console represents at least a convenience and at most a significant increase in productivity. This research focuses on the benefits discussed below; however, other benefits exist that fall beyond this paper's scope.

1. Flexible Demand

One of the most notable benefits of this concept is the flexibility to support higher demand (i.e., assuming a lower cost system translates to less procurement policy restrictions. For example, assuming the total expenditures for SME PEDs is about \$75M (i.e., cost to the government for R&D, upgrades, production, etc., not including the network operator charges, infrastructure, or security middleware cost) the manufacturer option, listed in the cost section, could support a much higher volume of devices for the same amount of expenditures. As mentioned in that section, the manufacturer would bear the initial burden of the R&D cost and potentially relay the cost to the end customer. This option provides the DoD a larger market to share the burden of the new technology.

2. Reduced Risk of Handset “Jailbreak”

A high assurance platform foundation could facilitate a policy that limits the ability to circumvent the security controls in a handset. For instance, the iPhone “Jailbreak” story provides an example of a vulnerability that is potentially preventable with a correctly implemented security architecture. Essentially, a jail-broken device is no

longer restricted to the policies the network operator and handset manufacturer implement. In the iPhone case, the device was designed to only operate on the AT&T network; however, after a phone is jail-broken, the phone can then be configured to operate on other networks, install third-party applications, customized ring tones, etc.⁷¹ The benefit received from the reduction or elimination of this vulnerability in a smartphone is a function of the impact (i.e., in the handset case, the cost of the device, the information contained on the device, and the networks that the device can potentially compromise).

3. Classified Mobile E-Mail Cost Savings

Currently, non-SME PED users are required to access their classified domains from a secure facility with wide area network (WAN) connectivity into the DISN. From the authors' perspective, the capability to remotely access SIPR or JWICS e-mail accounts while on the move provides a significant savings in travel time. The current SME PED devices provide this functionality, but only for a few thousand users. A lower cost COTS CDS device could facilitate defense-wide adoption, yielding growth in the number of users to hundreds of thousands or potentially millions. In this example, the time saved is the amount of time it takes to travel (including system login and application startup time) to and from the secure location. Using this example, it is possible to estimate a total savings in recovery cost from loss of productivity or opportunity cost.

In order to estimate the total cost per hour of employees' time, the authors used a statistics program (i.e., Oracle's Crystal Ball) to simulate the cost based on FY2011 DoD end strength distribution by pay scale.⁷² Since the purpose of this model is to illustrate potential cost savings and not holistically portray the actual benefits, the authors used only active duty personnel end strengths and pay scales. If this model were to capture all of the DoD's savings, the model would need to account for the end strength and pay of civilian, reservist, contractor, and other personnel.⁷³ Since this example accounts for only

⁷¹ Cassavoy, Liane. 2010. "What Does It Mean to Jailbreak an iPhone?" About.com. http://cellphones.about.com/od/glossary/f/jailbreak_faq.htm.

⁷² These authors used Oracle's Crystal Ball Statistic program.

⁷³ Reference Appendix D for actual end strengths and pay scales used in analysis.

cleared personnel (i.e., those who hold a clearance), the model estimated the lowest paid service member's hourly rate (i.e., E-5 at \$25 per hour considering secret-level clearance) and the highest paid (i.e., O-10 at \$117 per hour), then varied the expected rate based on the FY2011 end strengths distribution—the observed distribution closely matched a gamma distribution.⁷⁴ Since the authors estimate the current SME PED demand at about 2,000 users, the lower limit on demand was set at this constant. Since the total end strength of E-5 and above is about 783,000 personnel, the demand's upper bound was set at this constant. The simulation varied the demand, based on a triangular distribution, with 100,000 being the most likely demand. The authors assume that the ceiling on the demand currently enforced by policy will likely change once the devices become cost efficient. Since the current unclassified cellular demand for DoD is estimated at greater than 300,000 subscribers, the authors assume that if the devices approved for connecting to classified domains becomes cost efficient, the demand could significantly increase.⁷⁵

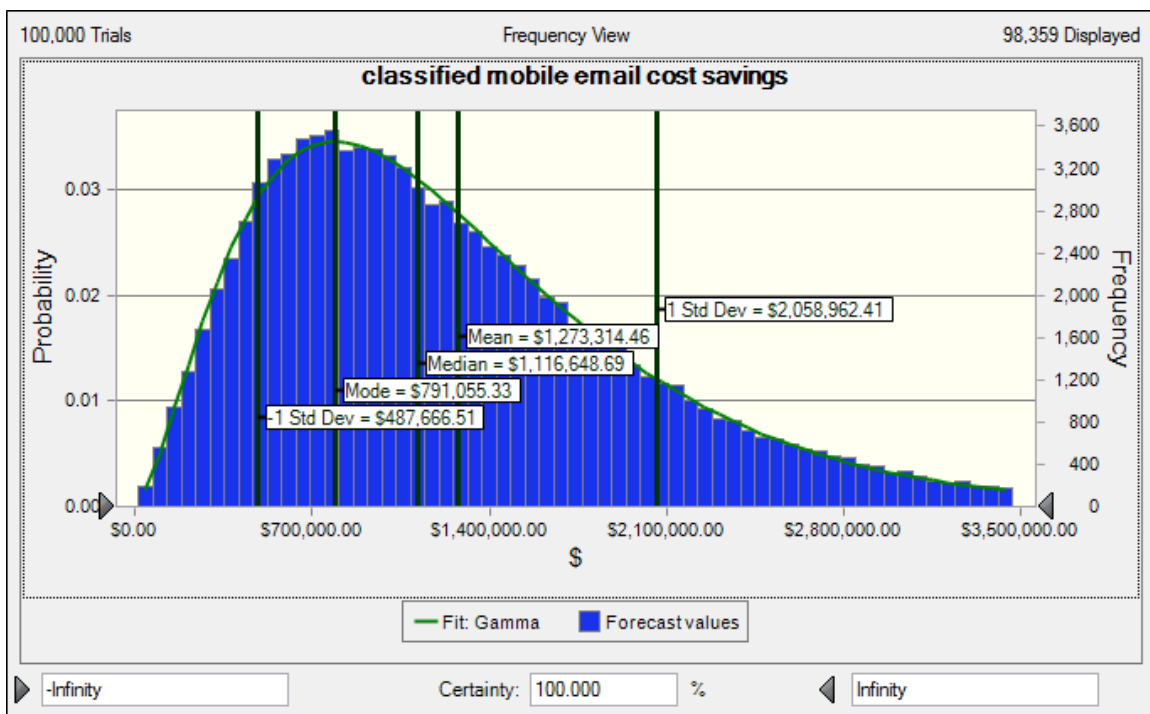


Figure 19. Potential Cost Savings for Mobile Classified E-Mail

⁷⁴ Rates and end strength totals referenced from individual services FY2011 budgets.

⁷⁵ Chapter IV provides the analysis on the demand.

Figure 19 illustrates the results of the simulation after 100,000 trials. The mathematical mode of the results indicates that the most likely potential recovery is about \$791K. This assumes each person can save between 1 to 10 minutes of productivity by having his or her classified e-mail messages on his or her hip rather than in a remote classified facility—of course, each individual case could vary drastically depending on his or her location relative to the facility. In the mobile classified e-mail simulation, the most likely daily recovery cost is \$791K (i.e., for 10 minutes of saved productivity) multiplied by 240 working days in a year results in an annual recovery of \$190M (NPV of \$363M considering 2 years' life cycle of the device with a 3% discount rate). Alternatively, Figure 20 illustrates the data from a different perspective (i.e., reducing the probability from including all cases).⁷⁶ The blue portion under the curve indicates that—under the same productivity assumptions—adoption of a COTS CDS smartphone affords the DoD, within a 95% probability, a recovery of at least \$428K per day or \$73M per year in opportunity cost (i.e., the next high-valued alternative).

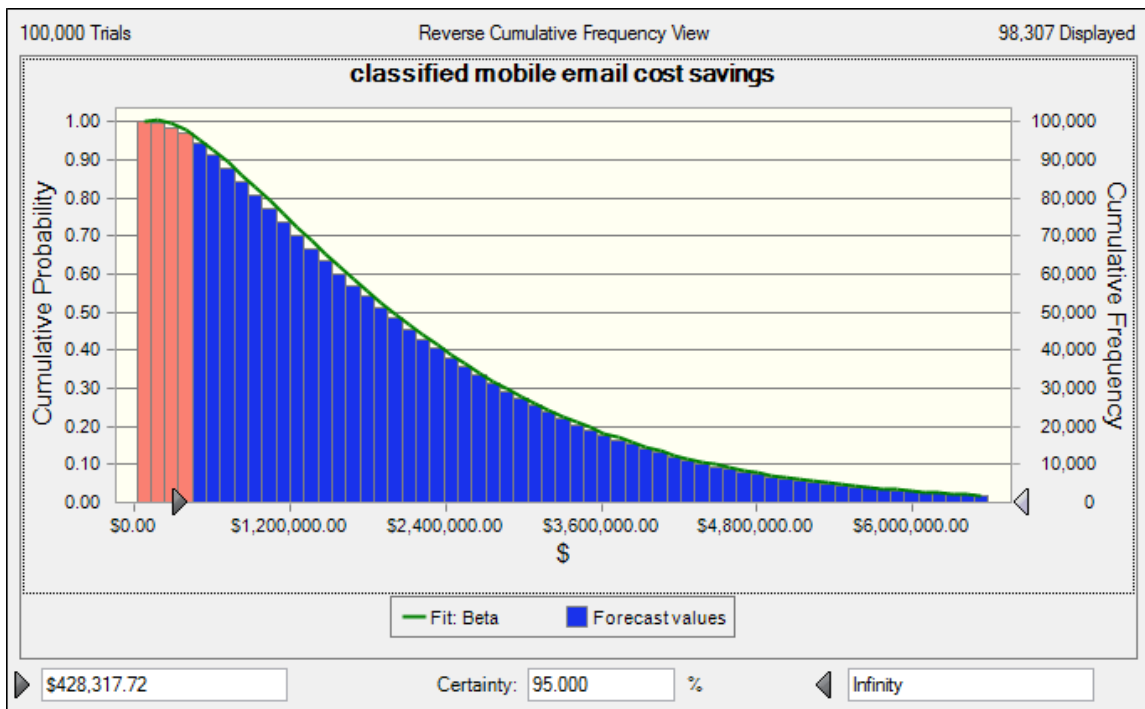


Figure 20. Minimum Potential Cost Savings

⁷⁶ Notice the differences in the certainty value and the y-axis labels between the graphs.

4. General Productivity Increase

Productivity increases seem debatable, depending on the various researchers and analysts. Some researchers and analysts report an increase, and others report a marginal decrease, in productivity from the use of smartphone technology. For example, the research firm Basex conducted surveys and interviews to establish the cost of interruptions. They categorize interruptions as either active (i.e., personal choice) or passive (i.e., external interruption—e-mail, phone, text, etc.). Of these interruptions, the respondents rank the most acceptable interruptions as supervisor needs immediate response, and colleague, subordinate, or friend/family member has a question. As a result of these interruptions, their research found 28% of a typical workday was wasted (Feintuch & Spira, 2005). Another survey from MIT highlighted some benefits of smartphones as an increase in mobility and a medium for communications during down time (Mazmanian, et al., 2006). Conversely, the survey highlighted the disadvantage of an increase in stress from the expectation of an increase in response time—supervisor expects immediate response (Mazmanian, et al., 2006). Essentially, the smartphone provides a medium for constant connectivity regardless of location and, therefore, should provide the flexibility to respond to inquiries at a faster rate. Alternatively, another research firm, Bay Street Group, reported 83% of their surveyed respondents agreed that the smartphone provided an increase in personal productivity. The respondents said the smartphone gave them the ability to instantly access information and rapidly convey the responses to clients, resulting in less wasted time and faster responses to customer questions (Telberg, 2007). Another report from the Ipsos Reid firm quantified the advantages of smartphones as a function of productivity increases. The report surveyed over one thousand BlackBerry users and over one thousand information technology managers who supported from 1 to 500 devices within their respective organizations. The report concluded two major findings (Moro 2007):

- A typical mobile user converts 60 minutes of downtime per day into productivity.⁷⁷

⁷⁷ This number represented the median of responses and is considered a typical user, because it was more conservative than the mean (i.e., 63%).

- Operations staffs have more time in their schedule than executives and, therefore, have more potential to recover more downtime.

Figure 21 represents the distribution of responses (Moro, 2007)

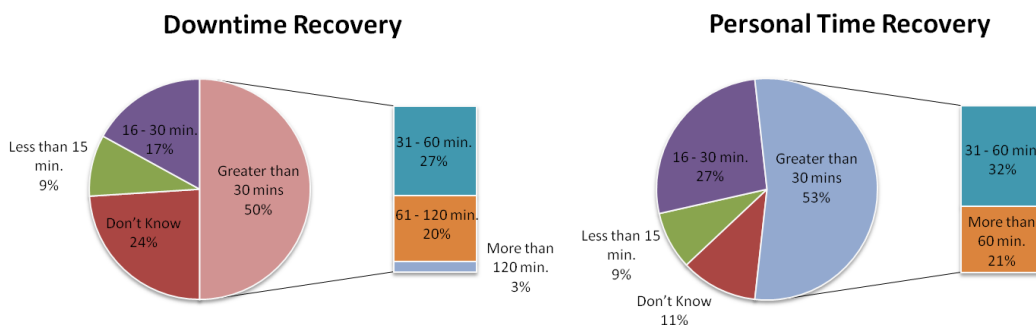


Figure 21. Productivity Recovery Potential (From Moro, 2007)

Section 3, “Classified Mobile E-mail Cost Savings,” assumed most users would use the device for reading and sending their classified e-mail. Since a CDS smartphone would theoretically have a number of capabilities other than mobile e-mail, this example assumes these added capabilities could save at least 1 minute and at most 10 minutes of productivity independent of what domain the user accesses. This assumption is based on the knowledge that approximately 90% of DoD employees currently lack the ability to use official smartphones for their daily work activities.⁷⁸ The authors recommend future research to focus on determining the DoD-specific marginal increases in productivity from using a smartphone device for official business. For this example, the statistical model varied the productivity savings from 1 to 10 minutes with a uniform distribution. The total number of users varied from 200,000 (minimum), to 340,000 (most likely), and to 400,000 tsubscriber (maximum) demand. These numbers were derived based on estimated DoD demand for cellular services and the maximum number of active duty employees. Again, this number could greatly increase if the model included civilians, reservists, contractors, etc. The hourly rate per employee ranged from \$16 (i.e., E-1) to \$117 (i.e., O-10) based on the different service’s FY2011 estimated end strength

⁷⁸ Conservatively estimate 300,000 current DoD wireless subscribers proportionately to 3M DoD employees.

distributions.⁷⁹ Figure 22 illustrates the results of the simulation after 100,000 trials. The mode, \$679K, indicates slightly less savings than the previous examples.

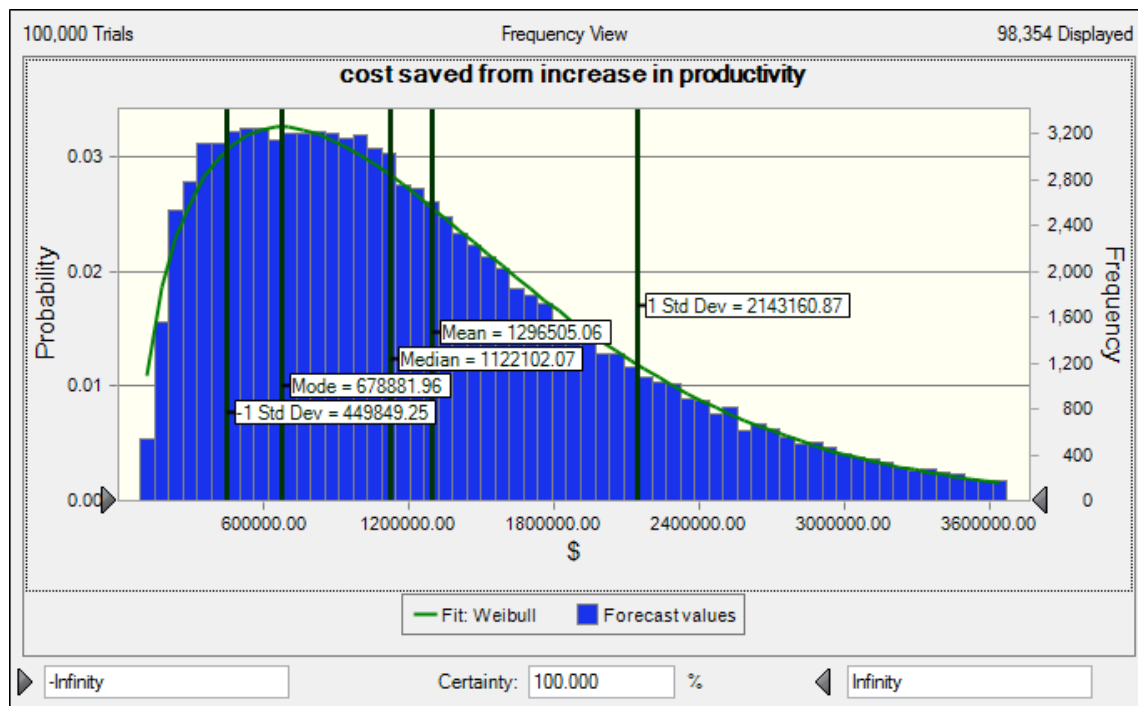


Figure 22. Potential Cost Savings for an Increase in Productivity

Given the few minutes of potential daily savings in productivity, the resulting opportunity cost is most likely \$679K a day or \$163M annually, which is a little less than the previous e-mail example. This example is likely more realistic because this model accounts for the total DoD population (i.e., a significant amount of comparatively lower paid employees). The previous model only included the personnel with a clearance and the authorization to have a secure smartphone (i.e., on average they are higher paid than the general population). Figure 23 illustrates the data from a different perspective (i.e., a reverse cumulative frequency view that provides probabilities). Under the same productivity assumptions, if the DoD proliferates smartphone usage throughout the organization, the blue area under the curve indicates that the DoD has a 95% probability of recovering at least \$277K per day or \$66M per year in opportunity cost.

⁷⁹ Rates and end strength totals referenced from individual services FY2011 budgets depicted in Appendix D.

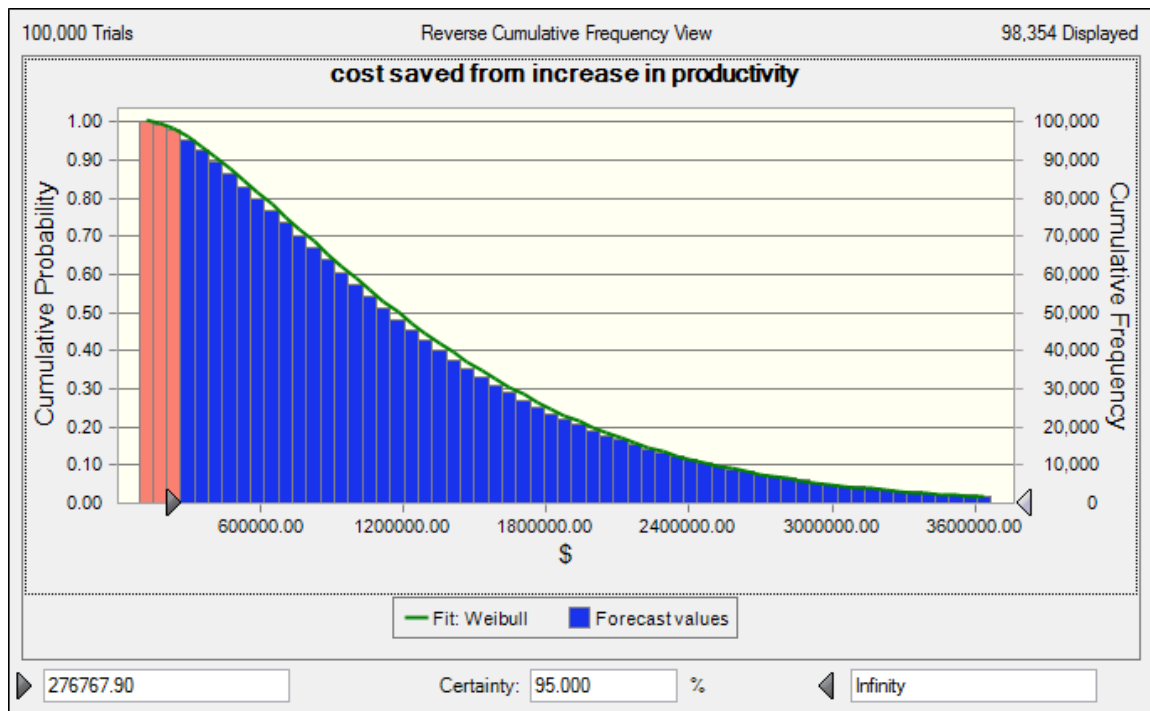


Figure 23. Minimum Potential Saving for Increase in Productivity

5. Reducing DISA Security Technical Implementation Guides Cost

According to policy outlined in DoDD 8500.1, DoDI 8500.2, CJCSI 6510.01, AR 25-2, and AFI 33-202, DISA is required to develop and provide security configuration guidance for IT systems. The current process for developing new Security Technical Implementation Guides (STIGs) can take a significant amount of time, depending on the inherent security vulnerabilities within any given system. A STIG is essentially instructions or procedures on how to configure a system in line with a baseline level of security.⁸⁰ The cost of the STIG process is a function of development, implementation, and opportunity cost.

- STIG development cost—the number of labor hours times the personnel cost.

⁸⁰IASE website: <http://iase.disa.mil/stigs>.

- STIG implementation cost—number of labor hours for local telecom offices to read, interpret, and implement the STIG configuration times the number of different systems configured.
- Opportunity cost—cost of not utilizing the technology to maximize mission effectiveness (e.g., the DoD releases a STIG for iOS products one year after the first commercial market availability—ultimately stifling operating cost, productivity, etc.)

The potential high assurance virtualization architectures could reduce the time required to produce a STIG for future mobile systems. Figure 24 illustrates the STIG process. The actual STIG development time varies based on individual IT systems. For example, even though personnel are working to finish an iOS and Android STIG, as of March 1, 2011, the STIGs still are not completed. Alternatively, if the DoD adopted these operating systems without an approved configuration, more vulnerabilities could exist.

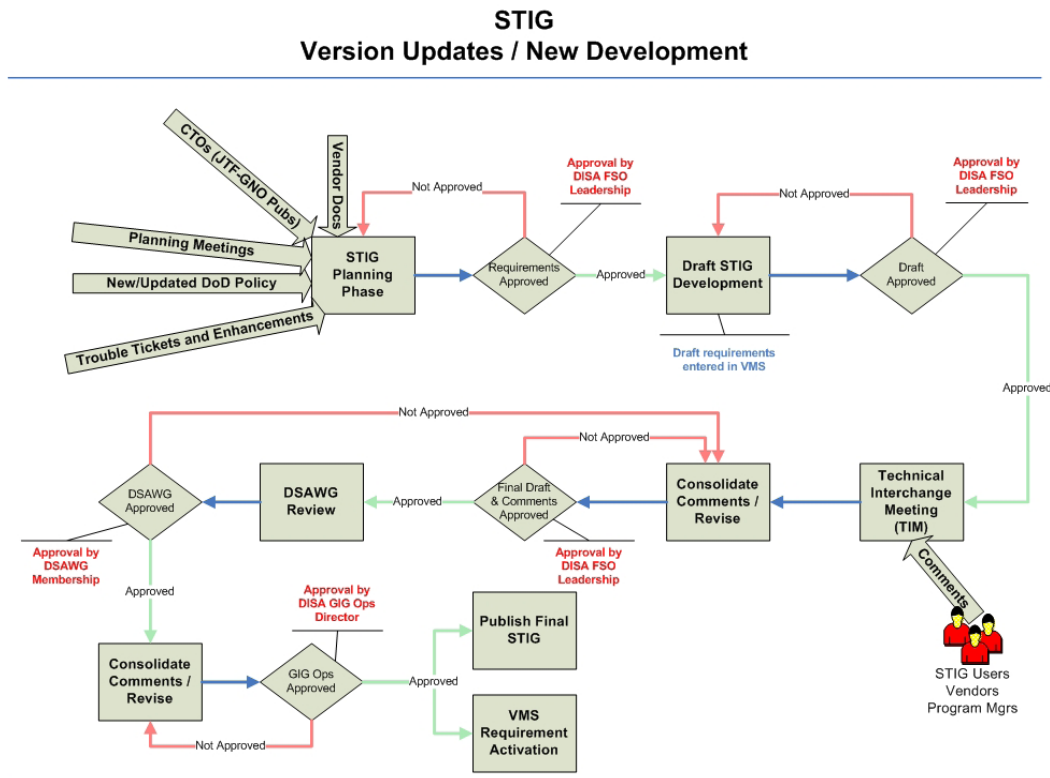


Figure 24. DISA STIG Process (From Defense Information Systems Agency, 2010)

6. COTS Option Value

A benefit not easy to quantify without further research is the concept of commercial solutions providing large option values. The SME PEDs were created to have specific capability sets where COTS smartphones are created with unknown capability sets (e.g., the idea of 3rd party application developers designing new innovative capabilities independent of the handset manufacturer's original intent). From a security perspective, this extensibility becomes a significant concern, since not all developers are equal. For example, a nonmalicious software programmer could ignorantly include vulnerable code or unintentionally introduce bugs. Alternatively, a malicious programmer could embed devious or potentially criminal code.

D. RISK

In an effort to evaluate the risk associated with the different smartphone architectures, this paper leverages the following equation: Risk = Vulnerability x Threat x Impact.⁸¹ As described in Chapter II and Appendix A, risk is a function of the vulnerability, the threat, and the total impact of potential compromise. In an attempt to relate a vulnerability score to current OSs, the authors assume that the OSs with higher EALs have more security controls to protect against threat events. Table 8 highlights a few OSs and their associated Common Criteria assurance levels. Not all OSs listed are available for mobile smartphones.

⁸¹ Refer to Appendix A for a more thorough discussion surrounding the risk equation and methodology.

Vulnerability (Operating System⁸²)	CC	Scale⁸³
Apple Mac OS X 10.6	EAL3+	.50
Windows Mobile 6.5	EAL4+	.36
Windows XP	EAL4+	.36
BlackBerry Device Software 5.0	EAL4+	.36
BAE XTS-400	EAL5+	.21
Green Hills Software INTEGRITY 178B	EAL6+	.07

Table 8. Operating System Common Criteria Categories

For this section, the smartphone device is considered independent of the connecting network. The threat and impact variables are considered constant across the various OSs, leaving vulnerability as the only variable. Since this approach only varies the vulnerabilities based on the properties of the OS, this paper only considers the technical vulnerabilities for the handset BCA. Therefore, risk is a function of the level of assurance of each OS. This paper uses an OS's EAL as a tool to measure and rank its level of assurance.

Since this chapter focuses on the costs and benefits of a standalone handset, the impacts and threats are considered constant. The value for impact is a function of the handset cost, and the cost of the information contained on the device. As defined in Appendix A, the value for threat is a function of the potential for an event to occur. Since this business case only recommends a variation in the technical approach (i.e., CDS vice commercial standard), these values are held constant (i.e., impact and threat = 1). Therefore, risk is equal to vulnerability (i.e., Risk = Vulnerability x 1 x 1). Based on this reasoning, a lower CC rating yields an inadequate system for higher risk environments.

⁸² Nonmobile device operating systems were included to provide a frame of reference.

⁸³ Scale = (Max CC score – CC score) / (Max CC score).

E. SENSITIVITY ANALYSIS

As previously discussed in Section C, Paragraph 4, a mobile device with a CDS capability can potentially provide increases in productivity. To quantify a range of potential opportunity costs, Table 9 enumerates the associated cost per minutes of time. Table 9 uses the same assumptions and methodology as Section C, Paragraph 4; however, this example varies the amount of recovered productivity time. For example, a mobile subscriber recovers 10, 20, 30, or 60 minutes a day from a weather application on his mobile device, instead of sitting through a 60-minute news show. A military commander receives intelligence updates through a personally customized widget application on his secure smartphone instead of through a 60-minute staff brief. This example varies the number of subscribers between 300K and 400K and assumes every subscriber can recover the same amount of productivity within the row threshold (i.e., gap of minutes). The expected (per day or annual) columns list the amount of opportunity cost the DoD could expect to recover. The minimum (per day or annual) columns show, with a 95% confidence level, that the DoD could recover at least the amount listed.

300K to 400K subscribers (FY2010)				Expected 340K
Productivity Increases	Expected (per day)	Expected (annually)	Minimum (per day)	Minimum (annually)
1 - 10 Mins	\$ 678,882	\$ 162,931,680	\$ 276,768	\$ 66,424,320
11 - 20 Mins	\$ 2,633,840	\$ 632,121,600	\$ 1,458,187	\$ 349,964,880
21 - 30 Mins	\$ 4,180,651	\$ 1,003,356,240	\$ 2,563,484	\$ 615,236,160
31 - 60 Mins	\$ 7,785,020	\$ 1,868,404,800	\$ 4,717,347	\$ 1,132,163,280

Table 9. Productivity Savings for 300K to 400K Subscribers⁸⁴

Table 10 uses the same assumptions, but it shows variation of the number of subscribers that could recover opportunity cost. This table assumes a gamma distribution for the number of subscribers who could recover opportunity cost. For example, not every person in the DoD might be able to recover the same value. A gamma distribution weights more occurrences toward the left—it is more likely to have 10%, 20%, or 30% of subscribers recovering opportunity cost rather than 100% (i.e., Table 9 illustrates the

⁸⁴ Appendix H includes the remaining tables.

recovery opportunity based on all subscribers receiving the same amount). Given these assumptions, the DoD is more likely to recover costs similar to those displayed in Table 10; however, Table 9 is worth evaluating if the entire subscriber base can recover an equal amount of time. For example, if all subscribers used the Exchange e-mail service, and each one could recover 10 minutes of time, then Table 9 applies. However, if the subscribers have unique applications that save these individuals time, then Table 10 is more representative of the recovery cost.

1 to 400K subscribers (FY2010)		Gamma Distribution		
Productivity Increases	Expected (per day)	Expected (annually)	Minimum (per day)	Minimum (annually)
1 - 10 Mins	\$ 94,776	\$ 22,746,240	\$ 38,030	\$ 9,127,200
11 - 20 Mins	\$ 423,422	\$ 101,621,280	\$ 162,115	\$ 38,907,600
21 - 30 Mins	\$ 731,530	\$ 175,567,200	\$ 274,357	\$ 65,845,680
31 - 60 Mins	\$ 1,238,500	\$ 297,240,000	\$ 470,253	\$ 112,860,720

Table 10. Productivity Savings for 1 to 400K Subscribers⁸⁵

Another question of interest is how much does antiquated technology cost the DoD over time. The results illustrated in Figure 25 use the same assumptions in the previous examples, but vary the amount of productivity across the years with constant increases in the subscriber base (i.e., the data is based on an unknown subscriber base). The authors assume the increase in subscriber base will follow the same DoD trends as the past 6 years.⁸⁶ The lines represent the amount of minutes recovered from an increase in productivity. Figure 25 illustrates the minimum amount of potential savings.

⁸⁵ Appendix H includes the remaining tables.

⁸⁶ Reference Chapter IV for DoD cellular demand trends.

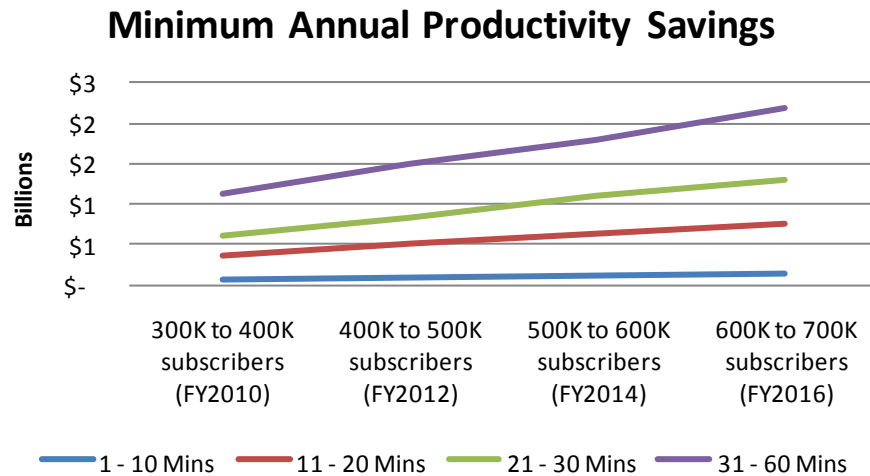


Figure 25. Cost of Antiquated Technology (Uniform Distribution [in U.S. Dollars])

Figure 25 assumes all subscribers receive the same level of productivity increases. However, the authors assume the subscriber base will receive a varied savings (i.e., gamma distribution) rather than a constant savings (i.e., uniform distribution) used in Figure 25—as in the user-specific application example where the individuals choose unique applications to meet their specific requirements. This assumes fewer subscribers will actually receive any savings from the added capabilities. Figure 26 represents the estimated FY2016 probability distribution (gamma) of subscribers who are expected to receive an increase in productivity from leveraging capabilities resident in smartphones.⁸⁷ The horizontal axis represents the number of subscribers. The vertical axis represents the likelihood that those subscribers will receive a productivity increase. Of 700K total subscribers, about 100K are most likely to receive a productivity increase.

⁸⁷ Figure 23 represents the estimated FY2016 DoD subscriber demand of 700K.

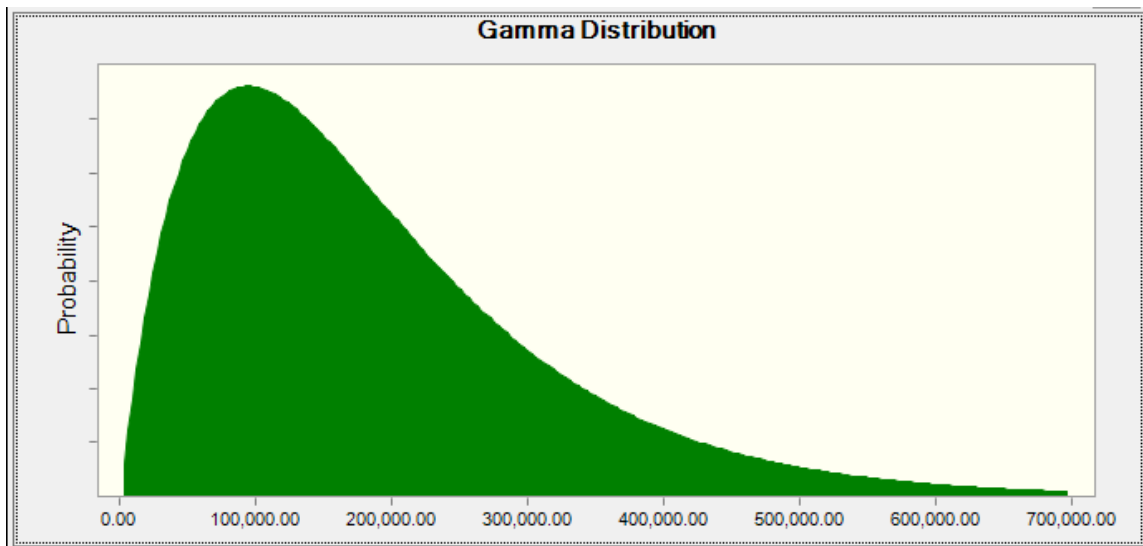


Figure 26. Expected Distribution of Subscribers Who Receive Productivity Increase

Figure 27 illustrates the same productivity model represented in Figure 25; however, it applies the gamma distribution illustrated in Figure 26. The results appear more realistic because the authors assume a significant number of subscribers will not realize any productivity increases from using a mobile device.

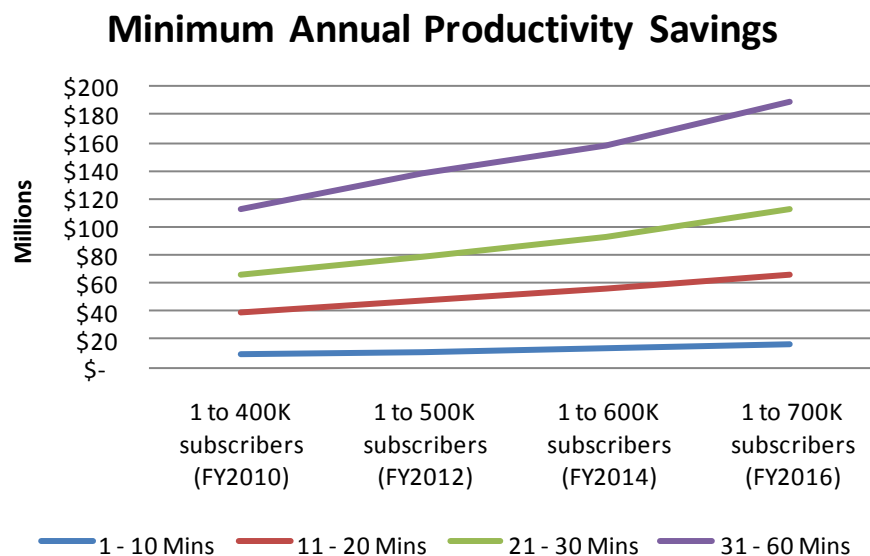


Figure 27. Cost of Antiquated Technology (Gamma Distribution [in U.S. Dollars])

In conclusion, from the productivity models, the authors estimate that a significant amount of opportunity cost is recoverable from larger procurements of smartphone devices. When considering the marginal productivity increase, the authors found that current subscribers are less likely to receive an increase in productivity—the current subscribers most likely already recover the lost time. However, since the unclassified domain receives an estimated demand of 10% saturation (i.e., as of FY2010, 340K subscribers among 3M employees), the potential for recovery exists as the subscriber base increases by up to 90%. Since the current demand for secure smartphones (SME PEDs) is extremely low in comparison to the total population, the potential for secure communication productivity increases is also high.

F. SUMMARY

In quantifying the net present value (NPV) for the various solutions, the authors assume that the previous or future R&D expenses are fixed and, therefore, negligible in comparison. Even though the SME PED program costs the DoD about \$44M, and the proposed COTS CDS is estimated at \$10M, the authors consider the recurring costs as the drivers of the NPV. As stated in the beginning of this chapter, if the DoD can leverage the commercial market's economies of scale, a COTS CDS smartphone is estimated to have a cost similar to that of BlackBerry devices. A comparison is presented in Table 11. Since the network costs are required to accurately calculate the TCO NPV, the COTS CDS versus SME PED comparison is included Chapter V.

Component	Annual Cost ⁸⁸	Component	Annual Cost ⁸⁹
SME PED Device	\$2000	COTS CDS Device	\$183
MCEP	\$900	Annual Upgrade	\$2
Apriva Server	\$150		
Upgrade cost	\$625		
Total	\$3675	Total	\$185

Table 11. Device Comparison

The authors assume the software licensing fees, and potential additional server costs, are negligible as the commercial market economies of scale offset the cost. The break-even mark for quantity is a function of the cost for the current SME PEDs. Table 12 highlights the quantity of potential devices under the same amount of funding allocated for the SME PEDs. Additionally, Table 12 highlights the potential quantity of devices as a function of productivity benefit.⁹⁰ Higher benefits are possible—especially since some of the research suggests productivity increases in the amount of 60 minutes. However, the authors chose a more conservative comparison by using a gamma distribution of demand, resulting in receiving between 21 and 30 minutes of savings per day.

	Unit Cost	Qty	Total Cost
SMEPED	\$3450	1500	\$5,512,500
COTS CDS	\$185	37,297	\$5,512,500
CDS Benefit			\$78,709,200
COTS CDS	\$183	425,455	\$78,709,200

Table 12. Device Cost Benefit Comparison

⁸⁸ Amortized across expected 2-year lifetime.

⁸⁹ Amortized across expected 2-year lifetime.

⁹⁰ Productivity benefit considers at least 20 mins per day leveraging the gamma distribution model.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. BUSINESS CASE ANALYSIS FOR LEVERAGING MOBILE VIRTUAL NETWORK OPERATOR SERVICES

Figure 15, in the previous chapter, provides an illustration of the desired characteristics for the business cases. This chapter evaluates a business case for implementing services typically managed by network operators (i.e., MNO, MVNOs, or MVNEs) in an effort to reduce cost from the current implementation, increase signal coverage (i.e., add functionality), and increase security functionality (i.e., reduce risk). The proposed business case leverages edge networks that operate on commercial licensed, unlicensed, and government reserved spectrum. This analysis seeks to identify a system that is capable of providing a high level of security and functionality at a low cost. For example, the various network architectures can provide additional signal coverage, enhance data services, or extended voice services where tactical communications become extended into commercial networks.

A. BASELINE ASSUMPTIONS

Given the continuing government cost-cutting efforts, the authors assume the DoD's current policy for wireless procurements is not sustainable. The ensuing subsections describe the current wireless DoD contracts, associated expenditures with trends, wireless best business practices, and a potential framework to mitigate various inefficiencies.

1. Current DoD Contracts

The DoD leverages various contracts and agreements to purchase cellular services. In this chapter, the authors focus on the common reoccurring cellular services and device procurements. These contracts and agreements establish the base case or "AS IS" model in evaluating the DoD's cost for cellular services. The Army and Air Force leverage the Army Contracting Command (ACC), National Capital Region Contracting Center (NCRCC), and Information Technology E-Commerce and Commercial Contracting Center (ITEC4) to generate and maintain their wireless service agreements (i.e., the Army Air Force Blanket Purchase Agreement (AAFBPA)). The Navy and

Marine Corps leverage the Naval Supply Systems Command (NAVSUP), Fleet & Industrial Supply Center (FISC) to generate and maintain their wireless service contracts (i.e., the Nationwide Department of the Navy [DON] Wireless Contracts [NDWC]). Until recently, the Navy Marine Corps Intranet (NMCI) program office (PMW-200) procured the wireless services for Navy and Marine Corps commands with access to the NMCI network through the Electronic Data Systems (EDS) contract. According to a recent report, the future EDS contract will only include data card services, and as of fiscal year 2011 (FY11) all NMCI customers must rely on the NDWCs to support the DON wireless requirements (NMCI, 2010). These agreements and contracts only specify the terms and conditions of the procurements. The local contracting offices retain the responsibility to generate the tasking and delivery orders (i.e., for the indefinite delivery, indefinite quantity [IDIQ] contracts), which detail the specifics of the procurement and delineate the funding lines for deducting expenses from the requesting command.

Table 13 provides a list of the various contracts supported by the two main contracting offices (i.e., only for the noncontrolled cryptographic items (non-CCIs)). As mentioned in Chapter III, the SME PED contracts are separately accounted for under the NSA I851 program office.⁹¹

NAVSUP FISC (N00244) NDWC	ACC NCRCC ITEC4 (W91RUS) AAFBPA
N00244-05-D-0010 (AT&T / Cingular)	W91RUS-06-A-0001 (Verizon)
N00244-05-D-0011 (Sprint / Nextel)	W91RUS-06-A-0002 (Sprint/Nextel)
N00244-05-D-0012 (Verizon)	W91RUS-06-A-0003 (AT&T)
	W91RUS-06-A-0004 (T-Mobile)
	W91RUS-06-A-0005 (Cellhire)
	W91RUS-06-A-0006 (Worldcell, Inc)
	W91RUS-06-A-0007 (Skytel Corp.)
	W91RUS-06-A-0008 (Alltel Corp.)
	W91RUS-06-A-0009 (USA Mobility)

Table 13. Major DoD Cellular Service Contracts

⁹¹ The SME PED contracts are classified and not available for public release.

These contracts and agreements service all the major components within the DoD, including the Defense Telecommunications Services–Washington (DTS-W) customers. Even though these contracts provide a procurement medium for cellular services, they differ drastically in their design. The NDWCs are firm fixed price IDIQ contract and the AAFBPA is a Blanket Purchase Agreement (BPA)—where one is a contract and the other is an agreement. The advantage of these procurement vehicles is that they reduce administrative time and cost, delivery times, and ultimately streamline the process for high demand federal procurements (Compton, 2010). The IDIQ contracts require the government to quantify a lower and upper limit of supplies or services (FAR 16.504(a)). With this type of contract—such that the government is obligating a minimum amount of purchases upfront—by design, it provides negotiation advantages for facilitating a lower price (FAR 16.501-2(b)). Alternatively, the upper limit in a multiple contractor award could limit the flexibility of the government to purchase from the market-dominating vendor. Essentially, one vendor is favored over the others because that vendor provides a better service. Once this vendor reaches its upper limit threshold, its contract is locked from further tasking or delivery orders. In this case, the government is confined to ordering from the remaining vendors until the contract date expires. Although this paper does not focus on the performance of the contracting mechanisms, a DoD-wide strategy may be more advantageous to the DoD than three separate strategies. Refer to Appendix B for more details illustrating the trends of each contract and agreement. Understanding the difference between these two procurement methods is essential when comparing the DoD trends against the commercial market’s best business practices.

2. Current DoD Procurement Trends for Wireless (Mobile) Services

Figure 28 illustrates the combined expenditures over the past 6 fiscal years for the DoD contracts and agreements. The data is represented by fiscal years in an effort to align the results for comparison with the DoD budget. These procurement trends are consistent with DoD base budget trends. Since 2005, the DoD base budget has steadily increased (Department of Defense, 2010).

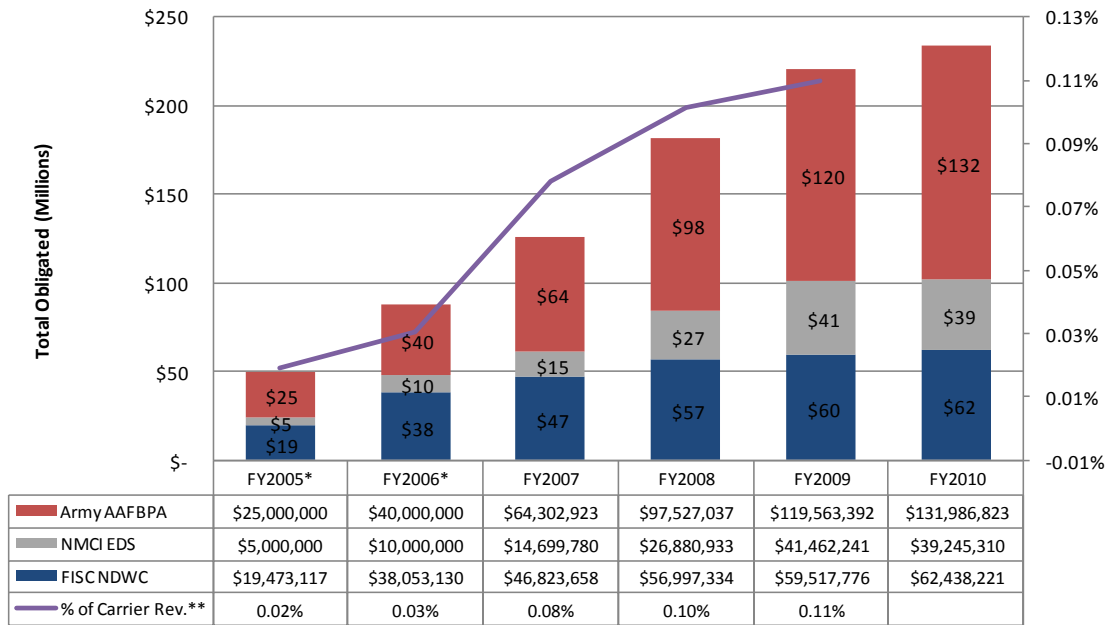


Figure 28. DoD Cellular Procurements^{92, 93, 94}

An important trend to note with Figure 28 is the rate of change over the past 6 years. The average expenses are increasing at a rate of \$40M per year (i.e., with an R^2 value of 0.9811). However, given that the wireless procurements are directly controlled by DoD policy, these trends are likely to continue until noticeable waste is identified and drastic organizational changes are made. For example, the EDS contract discontinued all wireless procurements possibly because of higher service cost in comparison to the NDWC.⁹⁵

Figure 29, illustrates the past 4 years of DoD procurement trends separated by the four major vendors. Only four vendors are depicted because they account for the majority of the procurements. Figure 29 trends are very similar to the commercial market share distributions (i.e., the top two network operators dominating the market with a combined

⁹² Contract totals obtained from extracting and aggregating the data from https://www.fpbs.gov/fpdsng_cms/ (Federal Procurement Data System – Next Generation) Addendum 1 – contains actual results.

⁹³ *FY2005 and FY2006 EDS and AAFBPA data are illustrated as estimates.

⁹⁴ **The FY2010 commercial carriers top lines were estimated since their financial records are not published.

⁹⁵ Refer to Appendix B for the contracts and agreements trends.

\$160M revenues from the DoD during FY2010). These close trend correlations are significant, because across the different contracts and agreements these correlations cease to exist. This suggests that as a single contract or agreement, the acquisition process might fail to provide adequate competition.

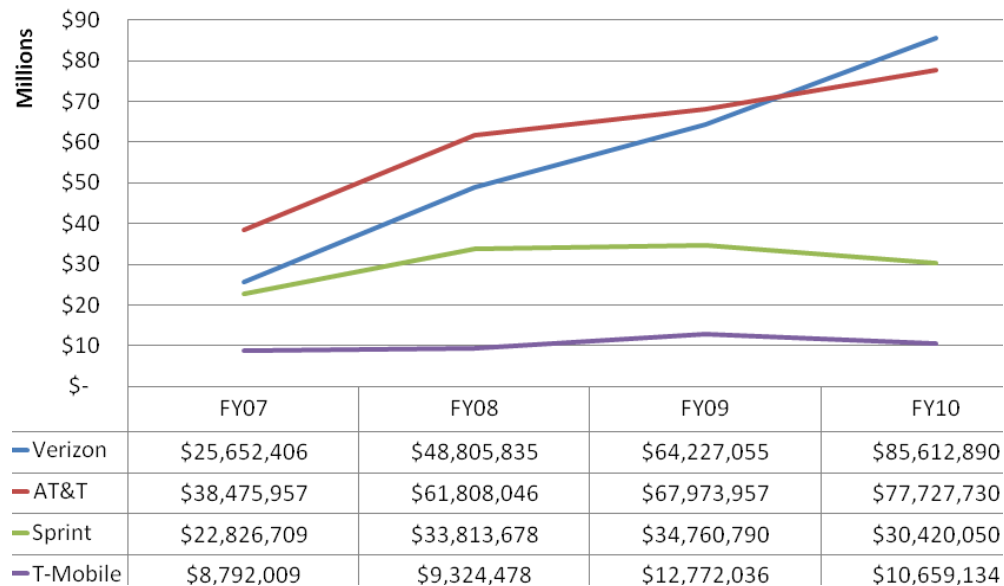


Figure 29. Breakdown of DoD Wireless Expenditures by Vendor

Based on FCC and CTIA data, the commercial annual ARPU was about \$565 in 2009 (FCC 2010). Since DoD procurement trends are similar to those of the commercial market, the authors assume a similar if not greater annual ARPU. In an effort to estimate the total annual DoD subscriber base, the authors calculated total annual expenditures divided by this commercial ARPU. This resulted in over 400K subscribers based on FY2010 expenses. Assuming the DoD uses more data and voice minutes than average commercial subscribers, this assumption decreases the estimated demand to 340K subscribers based on FY2010 expenses.⁹⁶ Therefore, the authors estimate DoD's (FY2010) wireless demand is between 300K to 400K subscribers. Using this same logic, Figure 30 illustrates the estimated demand from FY2005 to FY2017. The estimated

⁹⁶ DoD ARPU (\$680) is based on EDS (NMCI) accurately quantified demand and verified expenditures. In an effort to make the ARPU comparable across all contracts and agreements, the authors subtracted out the NMCI overhead from the EDS ARPU.

demand results in an average subscriber increase of 55K per year. However, this trend is not likely to occur, as policy will most likely limit procurements based on the increasing wireless cost.

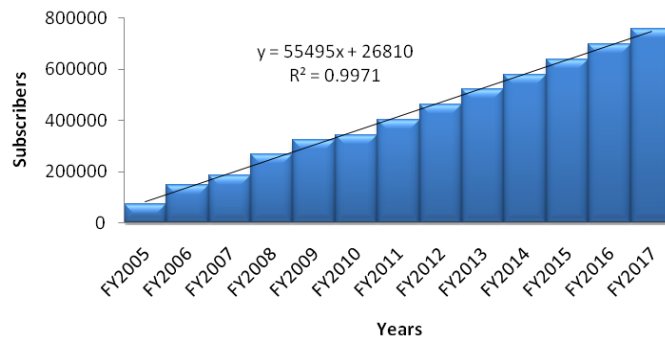


Figure 30. DoD Wireless Demand

3. Best Practices

The Aberdeen Group conducted a study between August and September 2010 that summarized the best business practices for controlling wireless expenses. The report reflects three major practices that the DoD lacks in their current procurement processes (Quickcomm, STS International, visage Mobility Central, 2010):

1. Automate the enforcement of contracts and policies,
2. Centralize the management of all devices, and
3. Track voice, data, and costs associated with wireless usage.

First, the DoD has auditing processes in place, but there are no tools for defense-wide proactive enforcement. For example, if the wireless procurement is under \$3000, the local contracting office could finalize the purchase without leveraging one of these contracts or agreements. In this case, the purchase is more difficult to track as a wireless procurement. In some cases, external contracting offices (i.e., other than the four military services), submit tasking orders against these contracts and agreements. Again, this is impossible to prevent, however, it is easily identifiable after the fact. No automated process exists to prevent out-of-contract procurements. Secondly, the DoD leverages two different offices, which use two different strategies for the contracts or agreements.

Therefore, holistically, the DoD does not have any process in place to centrally manage these devices. If the devices were procured against the NDWC or AAFBPA, and the contracting line item number (CLIN) referenced a handset, then at least the DoD could determine actual on-hand numbers by referencing the delivery orders. However, in most cases the handsets are either provided in conjunction with service—and therefore routinely not listed on the tasking order—or purchased through a general CLIN defining the purchase as a handset. Finally, since the local commands make the purchases directly with the vendors, it is not feasible to know about all of the devices purchased let alone managing or tracking usage. In an effort to estimate usage, the contracting offices request the individual vendors to supply quarterly reports but, when correlated with our known procurements (i.e., manually compiling the tasking and delivery orders submitted against these contracts), their data is drastically under reported.

According to a report from the Avotus Corporation, “Managing your Mobile and Wireless Spend,” they suggest developing a sourcing strategy by creating bucket plans, pooled minutes, or flat rate plans (Avotus, 2006). The pooled concept (i.e., tasking orders can pool their minutes to reduce overages) is common practice within the plans; however, the strategy still produces overage charges. The overage occurs when the usage exceeds the tasking orders’ combined limits. For example, five employees within the same command procure wireless services at the same time, under the same tasking order. These five employees have the option to pool their minutes under one plan. In this case, each employee is allocated 500 minutes per month. By pooling their minutes, the combined five employees share the 2,500 minutes vice their individual 500 minutes. The other strategy—contracting flat rates—mitigates the overage charges, but might be difficult to negotiate. If the DoD centrally contracted and combined the buying power, this flat rate might be more easily obtained.

As previously mentioned, the DoD is procuring wireless services from the vendors under the NDWCs, the EDS contract, or the AAFBPAs⁹⁷. The authors assume the tasking and delivery orders placed against these contracts and agreements represent

⁹⁷ The AAFBPA includes the DTS-W contracts.

the majority of the expenditures associated with providing the DoD mobile wireless access (i.e., via COTS smartphones and SME PEDs) to the DISN enterprise services from commercial cellular networks. The authors assume that the expenditures under \$3K (i.e., a credit card purchase and not included in contracts or agreements totals) are negligible since the cost of the device and associated annual service plan per customer is a significant proportion of the \$3K limit. Additionally, the authors assume the expenditures are negligible because the customers are incentivized to pool minutes in order to receive the highest value for the lowest cost. The expenditures include the handset cost—even though in most cases the handsets were provided (“free of charge”) with bundled procurements for wireless services. Currently, these contracts are negotiated from the perspective of the end users—where the services are grouped together by vendor and sold as a consumer product. Traditionally, this affords the DoD a fairly flat discount rate from the commercial market because of its large, semi-consolidated consumer base. Alternatively, the DoD could negotiate individual services (i.e., customer care, business to business, machine to machine, voice-mail, messaging services, etc.) based on the business case of outsourcing vice in-housing. This may provide the DoD a more substantial discount, facilitate more flexibility for integrating operational communications, and more control of wireless networks.

4. Mobile Virtual Network Operator Model

In an effort to assess a solution that potentially offers a lower cost for greater capability, this chapter evaluates the MVNO model. As explained in Chapter II, the commercial MVNO business model complements the MNO. In one case, the MVNO may provide services to otherwise underserved customers. According to an MVNO market research report, the MVNO industry differentiates their service offering according to the targeted customers demand (MindCommerce, 2010). Since the DoD has 3M employees, with an estimated 300,000 current subscribers and a unique requirement for tailored services, this MVNO model might benefit the department as long as the implementation does not result in the government competing with industry. Therefore, the DoD should investigate leveraging various commercially available services in the underserved regions. For example, Fort Knox, an Army base, is a region with comparably

less commercial cellular coverage than other military bases. Figure 31 illustrates the coverage maps copied from the corresponding network operator's website. Basically, the colors depict the various signal strengths. These figures represent the carrier's interpretation of their own coverage.

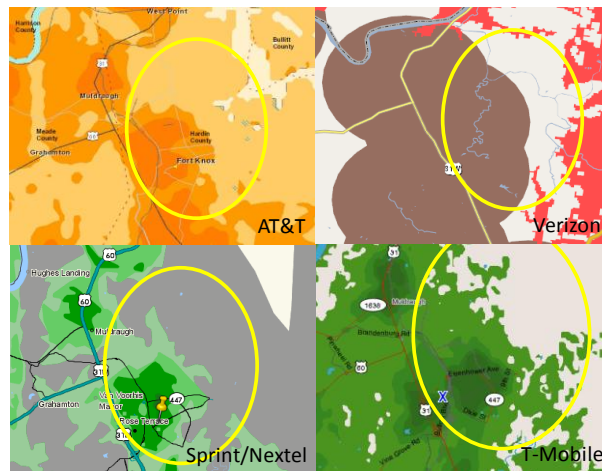


Figure 31. Network Operators' Coverage Maps for Fort Knox, KY⁹⁸

In this example, the DoD might consider requesting additional coverage from each of the network operators but, in some cases, the business case to support the additional equipment might not justify the expense. Another option is that the Army could purchase commercial grade base stations, outdoor repeaters, or indoor femtocells depending on the requirements. In the case of the Army purchasing the base stations, the Army would need to contract additional services in order to support the installation, operation, and maintenance of the equipment. Each of these options is commercially available and, in some cases, has already been implemented. Although each of these options meets one of the desired outcomes (i.e., increased coverage), they still fail to either reduce costs or increase security.

When evaluating the same problem from a global perspective, Figure 32 illustrates a reasonable representation of the GSM coverage. When considering the various cases for increasing coverage, this figure provides a high-level overview. The

⁹⁸ Network operator provided images.

areas that already contain commercial spectrum licenses provide the DoD with a significant opportunity to leverage the preexisting infrastructure and innovative technology advances. However, across a significant portion of the globe, commercially available coverage is completely missing.



Figure 32. GSM Worldwide Coverage⁹⁹

The DoD has over 3M employees, with some residing in underserved regions (e.g., military training areas, remote locations, operational deployments, etc.), and the cost for services are increasing at a rate of \$40M per year. The idea of the DoD providing MVNO service for employees might be worth exploring—especially in areas where the DoD receives inadequate coverage. Another use case is the deployed environment where the military services require a higher level of security assurance.

Figure 33 divides the various MVNO concepts into useful categories for evaluating the potential cost when considering a DoD implementation. For reference, Appendix G provides a technical overview of the integrated mobile network architecture.

⁹⁹ GSM world coverage map sourced from http://www.coveragemaps.com/gsmposter_world.htm.

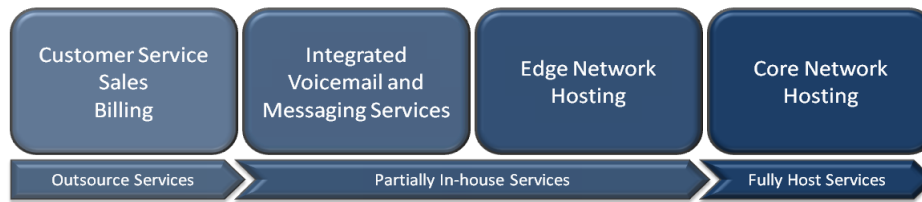


Figure 33. MVNO Divided Services¹⁰⁰

The following list describes Figure 33:

1. *Customer Service, Sales, and Billing.* The commercial equivalent of the function is a service provider or reseller. This is a fully outsourced business model in which the DoD would contract a third-party provider to host all cellular services. In this model, the DoD would provide the front-end customer service (i.e., similar to the current base telecommunication offices), a virtual store for sales, the billing function through inherent contracting offices, and the remaining services are outsourced.
2. *Integrated Voice-Mail and Messaging Services.* This model is similar to the enhanced service provider as described in Chapter II; however, in this model the DoD provides the messaging services. Potentially, DISA could add additional voice-mail and messaging servers or alternatively outsource the service depending on best value.
3. *Edge Network Hosting.* This model differs from the commercial MVNO model. As discussed in Chapter II, an MNO usually owns the spectrum and therefore retains responsibility for the edge network equipment. However, the DoD might require edge network control for austere environments, humanitarian support, disaster relief, or underserved domestic training bases.
4. *Core Network Hosting.* This model completely integrates all of the core network functionality under the MVNO. As discussed in Chapter II, some commercial MVNOs internally operate, maintain, and support core networks, but leverage other MNOs for the edge networks.

¹⁰⁰ Refer to Appendix C, for a full list of cost normally associated with MVNOs. Those line items were used as a basis for developing the following cost estimates.

B. MVNO COST ANALYSIS

1. Customer Service, Sales, and Billing

As previously mentioned in Chapter II, a significant number of MVNOs start as resellers or service providers—they buy wholesale cellular services from a strategic partner (i.e., MNO) and resell the services with the added value of better customer service, sales, or unique handsets. For example, this approach is similar to the original Boost Mobile, Consumer Cellular, Locus Telecommunications, Page Plus Cellular, Platinum Tel, and Qwest Wireless business models (H. White, 2010). As these MVNOs grow in customer base, the companies start in-housing services to realize more cost savings. For example, with a small amount of traffic, it is fairly easy to dedicate resources for that wholesale customer. However, once the customer base reaches a significant number of users, the traffic starts saturating the partitioned resources. Higher end switching centers can support millions of users, but if capacity is underutilized, the hardware costs and high fixed costs cannot be spread as far. This situation results in decreased operating margin. It seems reasonable that once a company's customer base reaches enough capacity to require a dedicated high-end core network, the MVNOs might either start in-housing the services to realize larger profit margins or merge with their partnering MNO. For example, Boost Mobile is no longer an MVNO, as they are wholly owned by their underlying network operator, Sprint Nextel. Given an open and competitive market, the large MNOs seem reluctant to provide ubiquitous cellular services, and therefore small niche markets arise from MVNOs. This is consistent with the sourced after action reports (see Addendum A)—government regulations required extended coverage areas for disadvantaged users; and therefore, the last 20% of coverage accounted for 80% of the cost.¹⁰¹

If the DoD desires to internalize various MVNO services, the first categories with which to evaluate attributable costs are customer service, sales, and billing. This is based on traditional MVNO startups, and it seems easiest to internalize without incurring a significant change in organizational structure. Since a significant amount of military

¹⁰¹ Given the sensitivity of this AAR, the Addendum is labeled as government distribution only.

bases currently contain telecommunication offices with customer service support for the wired telephony, it seems reasonable that these offices could support wireless customer requests. The authors note from personal experience that, some commands currently offer a significant number of services for cellular devices. For example, some commands receive devices from the providers, inventory the items, and contact the service provider to provision the devices prior to delivery to final customers. This added process allows the commands to track devices and arguably better manage their communications.

In the commercial market, considering a 200,000 to 1,000,000-member customer-base, the cost to provide the services in the first category (customer service, sales, billing, etc.) could range from \$5M to \$23M per year.¹⁰² The cost driver in this model is the labor cost. Although difficult to quantify, the number of employees required to support the subscriber base significantly affects the price. Since the added value of most MVNOs is an increase in customer support (i.e., as compared to MNOs), this model accounts for a customer-service-representative-to-user ratio of 1:5000, vice the industry standard of 1:10,000 users.¹⁰³ The majority of the cost associated with this category is the marketing cost (i.e., 40–62%). Assuming the DoD modifies the wireless policy by requiring all official wireless procurements to purchase services under this proposed model, the DoD could eliminate the cost of marketing—traditionally spent by the commercial market. Therefore, the tens of millions to hundreds of millions of dollars in marketing costs were not included. Since the DoD inherently maintains wireline services, the authors assume some level of wireless services support could come from the current facilities—especially if the wireless subscriber base increases and the dependency on wireline services decreases. The potential sunk cost associated with the current wireline customer service was not included in the final calculation. In addition to the front-end customer service, sales, and billing cost there exists a cost for the underlying commercial wireless network (i.e., the reselling part). The cost to procure the remaining cellular services varies drastically depending on the negotiated rate with the strategic wholesale partner. Based

¹⁰² Cost based on MindCommerce MVNO Business Case report from VIBE cost reporting and other market research.

¹⁰³ Industry standard referenced in MindCommerce MVNO Business Case report from VIBE cost reporting and other market research.

on a commercial provider's estimate of the remaining services required to support smartphone capabilities, and assuming the same customer base, the cost ranges from \$49M to \$180M per year.^{104,105} An additional capability of interest is the ability to tunnel communications through commercial networks in roaming environments. Since the SME PED program currently implements this functionality at a cost of \$2M per year (i.e., Apriva Multi-Carrier Entry Point [MCEP]), and other commercial providers offer this at an arguably reduced level of assurance for about \$500K per year. The authors assume the cost to add this functionality is estimated at about a couple million dollars per year. Therefore, the final cost estimated to support this category is between \$56M and \$205M per year. However, as the years progress and the DoD subscriber base increases toward 1 million users, the cost will increase toward the \$23M for the customer service, sales, and billing support. This trend will ultimately drive the wholesale cost for the underlying network beyond the annual cost of \$205M.

2. Integrated Voice-Mail and Messaging Services Cost

In some cases, the MVNOs attempt to differentiate their offered services by providing unique services. For example, Boost Mobile originally offered Boost Walkie-Talkie service including specialized wallpapers, games, applications, voice-mail greeting, and other customized services (H. White, 2010). Kajeet, a family oriented MNVO, offered parental management tools, a time manager, and a content manager to assist parents in limiting features on the children's handsets (H. White, 2010). Sti Mobile specialized in push-to-talk (i.e., with Sprint Nextel as the underlying operator), MMS, e-mail, and instant messaging (H. White, 2010). The idea is that the MVNO model provides the flexibility to specialize in the areas that the niche market requires. In the DoD's case, a specialized voice-mail (e.g., a single voice-mail that is permanently associated with each employee independent of their current phone number or attached command) or integrated messaging (e.g., an enterprise global access list with the ability to send SMS, MMS, or instant messaging without knowing the individuals phone

¹⁰⁴ Reference Addendum B for carriers provided wholesale cost (distribution restricted).

¹⁰⁵ Appendix C list additional services that were considered as remaining.

number—a DoD-wide phonebook searchable by name). The integrated messaging service could leverage a service similar to DISAs current enterprise directory service (i.e., Global Directory Service / Joint Enterprise Directory Service). These services provide the first steps toward a true ubiquitous mobile communication capability.

Based on a coalition partner’s MVNO business case (Addendum A) and past procurements of cellular infrastructure by Yuma proving grounds, the cost to purchase voice-mail servers, short message service (SMS), multimedia messaging service (MMS), and enterprise servers for hundreds of thousands of users could range from \$2M–\$4M and incur a \$200K per year cost for maintenance and support.¹⁰⁶ Using the same five-year range the NPV results in a cost of \$4.6M. This option considers purchasing the equipment and contracting out the maintenance and support. Although some additional fixed costs exist, the authors consider them negligible in order of magnitude (e.g., certification and accreditation).

Another option is to procure the services through a third-party vendor outside of the traditional major carriers. These third-party vendors—message aggregators—provide the interconnect between network operators. They facilitate delivering person to person (P2P) and application to person (A2P) messages between wholesale customers. For example, a P2P delivery occurs when a Verizon subscriber sends an SMS to a Sprint subscriber. An A2P delivery occurs when an advertising company sends mass SMSs to hundreds of thousands of subscribers across all the network operators. The military could leverage A2P services during disaster situations, for distributing recall messages, or publicizing command wide notices.

3. Edge Network Hosting Cost

As previously mentioned, the MVNOs usually defer the ownership of the edge network¹⁰⁷ equipment to the MNOs because the ability to propagate cellular signals requires either spectrum licenses or leasing agreements. From a technical perspective,

¹⁰⁶ Referenced sources are labeled as government distribution only; however, the data presented in this section is distilled into a public released format.

¹⁰⁷ See Addendum A for previous business case analysis. (distribution restricted).

this approach (i.e., hosting edge network devices) seems more valuable than owning the entire network. The military services travel worldwide to places that lack commercial signals including austere environments, international waters, and natural disaster environments. In these locations, the military needs the ability to leverage inherent communications devices.

When developing the concept of operations (CONOPS) for wireless communications, an important consideration to evaluate is the electromagnetic emission environment for the mission. Since spectrum is a finite resource with a high demand, and ownership varies by region, this requirement could limit the remaining available options. A number of other environmental conditions further restrict the options. For example: Is there an emissions threat? How austere is the terrain? How mobile is the operation? What is the number of users per area? What is the duration of sustainment without resupply?

Each region around the world drastically differs in the applicable policies and regulations for managing spectrum. Therefore, the business case for integrating smartphones into military operations must be adaptable to every potential environment. This section discusses the various integration concepts based on the potential wireless environments, which are allocated as commercial licensed, unlicensed, or government spectrum. The commercial licensed spectrum includes all frequency bands, which are allocated globally for mobile cellular communications. The unlicensed spectrum includes the globally allocated bands for wireless communications. The government spectrum includes all domestically and internationally allocated frequencies for military operations.

a. Commercial Spectrum

If an environment exists where emission security is not a concern and commercial spectrum is available, the DoD could leverage two different types of edge network concepts based on their mobility requirements. For example, on a domestic military base that is underserved with cellular coverage, the DoD might require fixed base stations to provide intranet-like services (i.e., the base owns and controls the entire network under an enhanced security policy). In this case, fixed commercial base stations

and controllers could satisfy the requirement. Alternatively, for military mobile operations (e.g., an on-the-move training exercise in areas without commercial cellular coverage) or rapidly deployable situations (e.g., disaster relief operations) the ruggedized mobile stations become desirable.

(1) *Radio Access Network*. In areas of lower commercial demand and therefore gaps in the cellular coverage, the DoD might require additional assets to transport government furnished equipment (i.e., DoD purchased smartphones) traffic. The required edge equipment can range from fully commercial-grade fixed base transceiver stations (BTS) / base station controller (BSC) or Node B (NB) / radio network controllers (RNC) to simple in-building repeaters or gap-filler picocells / femtocells (i.e., smaller sized base stations). In some cases, the fixed commercial-grade RANs (i.e., BSC/BTS/RNC/NB) will satisfy most CONUS operations. The cost to provide these assets can vary based on the required user capacity, RAN scalability, and procurement quantities. Table 14, illustrates the cost and lifetime of commercial RAN equipment based on data in Addendum A and correlated with Yuma proving grounds previous procurements.¹⁰⁸

Description	Quantity	Minimum	Maximum
BTS / NB ¹⁰⁹ (Macro/Pico/Femto)	1500–4000	\$45,000,000	\$180,000,000
Installation and Additional Material Cost		\$4,500,000	\$20,000,000
BSC / RNC	20–35	\$6,000,000	\$14,000,000
Total		\$55.5M	\$214M
Total per year (7 year lifetime)		\$8M	\$30.6M

Table 14. Standard Fixed Commercial RAN Costs

¹⁰⁸ Referenced sources are labeled as government distribution only; however, the data presented in this section is distilled into a public released format.

¹⁰⁹ Assuming 3 sections with 2 transceivers; costs can vary depending on manufacturer and size.

Table 14 highlights RAN equipment costs based on a concept of operations in which the devices are fixed to a specific location. The quantities represent a rough order of magnitude given the DoD's current estimated demand. Quantities greatly depend on the area covered and subscriber density; however, the ratio between BSC/RNC and BTS/NB should roughly remain constant. The equipment costs delineated in Table 14 are represented as an order of magnitude to support tens of thousands to millions of subscribers across varied distributions. Refer to Appendix G for the current DoD distribution of wireless procurements. The demand percentages in Appendix G are illustrated by region, based on the physical locations of the funding offices. In some cases, the illustration might be misleading because the subscribers continually travel and rarely remain stationary in one region. Therefore, the authors recommend a more thorough study be completed to determine a more accurate representation of wireless usage by region. The accuracy of that study could drastically reduce the variability of the projections in Table 14.

(2) *Ruggedized Mobile Base Stations.* Addendum D illustrates the costs and specifications of candidate ruggedized mobile RAN systems. Other variants are commercially available. The authors chose to list these variants, because of personal experience with purchasing the device and familiarity with the technical advantages and limitations.

Some of the equipment listed in Addendum D provides additional capabilities not found in the standard commercial equipment (i.e., SIP server, a Wi-Fi access point, MSC capabilities, etc.). However, all of these devices leverage the standard commercial cellular protocols and operate on the standard commercial mobile spectrum. These devices were developed for austere environments and marketed towards federal departments. The cost per subscriber is roughly similar to the fixed commercial equipment; however, in some cases the small size and ruggedization creates higher per-subscriber cost.

(3) *Spectrum Cost.* Since all of the devices mentioned in this section operate within standard commercial cellular protocols, the systems only operate on commercial spectrum. Therefore, when evaluating the TCO, the business case should

include the cost for leasing the spectrum. According to various MNOs, the vendors were willing to lease spectrum under two conditions: 1) the region of interest lacked cellular signals and failed to present a reasonable business case for adding additional coverage (i.e., limited demand); 2) the region of interest proved infeasible for establishing tower real estate (i.e., lack of geography for new towers). If either of those conditions were met, the price for leasing spectrum ranges from hundreds to tens of thousands of dollars per location, per month, and per frequency channel. In addition to the spectrum cost other costs can exist, but those special cases are not accounted for in the above examples. For example, other costs can include the cost for the power to run equipment, shipping and transportation, yearly maintenance and support, and labor hours for training new personnel on how to use the equipment.

b. Unlicensed Spectrum

Another option when considering wireless communications is unlicensed spectrum. From a cost perspective, this option is the most efficient solution (i.e., licensed spectrum requires fiscal expenditures to lease and government spectrum requires a loss in opportunity cost). Regarding availability, there exist many different COTS devices with the capability of facilitating communications across the unlicensed spectrum. Of the commercially available devices, Table 15 lists their various associated unlicensed bands according to the Federal Communications Commission (FCC) website.¹¹⁰

Frequency	Description	Standards	Max Power
902-928 MHz	ISM Band (GSM in some countries)		
2.400-2.4835 GHz	ISM Band	802.11b/g/n	4W
5.150-5.250 GHz	UNII	802.11a	200mW
5.250-5.350 GHz	UNII	802.11a	1W
5.250-5.350 GHz	UNII	802.11a	4W
5.800-5.925 GHz	ISM Band		

Table 15. Unlicensed Bands

¹¹⁰ Sourced from the NTIA website: <http://www.ntia.doc.gov/osmhome/allochrt.html>.

Of these unlicensed bands, this paper assumes a significant number of modern smartphones have the capability to connect to Wi-Fi access points. From a security perspective, the commercial signals fail to provide adequate protection against malicious attacks.¹¹¹ However, in some environments, a reduced likelihood of emission threats may provide an opportunity to leverage these bands. For example, within the United States, under FCC regulations, and within highly utilized public WiFi hotspots, the wireless service seems sufficient, otherwise the service would not exist. If the service was too slow or was continually interrupted, then perhaps other transport mediums would arise. In these areas, given the high demand, it seems feasible that the military could propagate signals across unlicensed bands without malicious interference.

(1) *Secure VoIP Via Tactical Network Extension.* Figure 34 illustrates a simplistic overview of a comparably inexpensive architecture to extend voice and data services to modern smartphone devices. This concept assumes that the phone is configured with a separation kernel and VMM capabilities to provide the user interface and additional layers of protection (i.e., assuming the device is certified with a high CC score).¹¹² This implementation assumes that the various operational use cases would consist of environments without emission control restrictions. In this instance, the Wi-Fi access points provide the bridge between the tactical network and the commercial protocol. Another assumption is that the smartphones host Suite B algorithms to encrypt all data prior to transmission. In this case, the wireless access points have the capability to decrypt the packets prior to routing through the tactical network. Although not considered in the below cost analysis, another option is to not decrypt the packets until they reach the PBX network.

¹¹¹ Refer to (Dixon, 2010) for a more in-depth discussion about signal vulnerabilities.

¹¹² Chapter III describes the separation kernel with VMM approach.

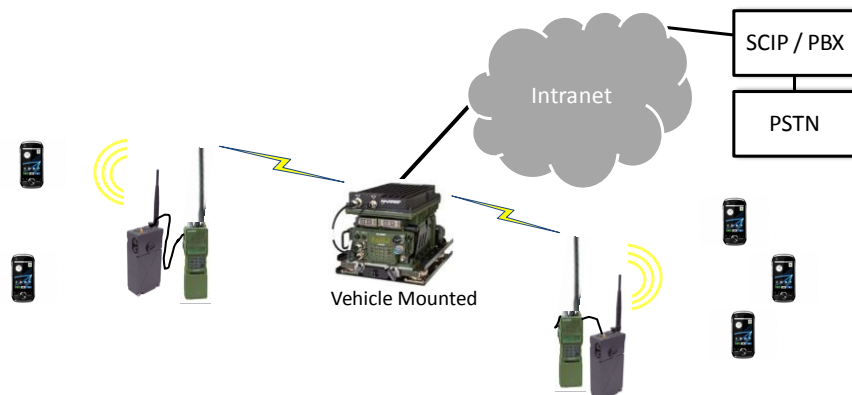


Figure 34. Wi-Fi Architecture

Figure 34 represents an architecture to leverage existing tactical communications networks. For fixed enterprise architectures, the radios are replaced by routers and switches, and the wireless access points are replaced with enterprise variants. Across all variations and architecture designs, the cost for this capability remains limited in comparison to previous concepts. The cost for the wireless access points depends on manufacturer and variant, but can range from \$500 to \$5,000 per device. Since each of the military services inherently has VoIP networks, and in some cases leverage the VoIP infrastructure to manage their wireline networks, the other required equipment (i.e., tactical radios, smartphones, PBX server, PSTN, etc.) is considered a sunk cost. The difficult number to calculate in this concept is the quantity. How many additional domestic wireless access points are required? How many deployable access points would the services require to support current and future operations? These questions are extremely difficult to answer, especially since the military services differ in their opinions of the CONOPS. For example, in a public wireless conference, an Army representative stated that every Soldier should have a smartphone device, and the Marine Corps representative stated only the squad leaders and higher should carry devices.

(2) *Secure / Unsecure VoIP Via Garrison Networks.* For garrison environments, the architecture is similar to that shown in Figure 34—where the Wi-Fi access points route the client handset traffic. However, for this use case the service members are located inside their command building or surrounding area. This concept assumes that the base provides a fairly high level of physical security to limit potential

threats. Additionally, this paper assumes emission security vulnerabilities remain negligible when physical security measures are enforced aboard continental U.S. (CONUS) military bases. For this use case, there are two architectures to evaluate. The first implements link encryption through similar Wi-Fi access points as listed in the previous section. The second architecture is purely a COTS Wi-Fi access point. This implementation adds no additional security measures to the standard Wi-Fi router. This is valuable because the access points are drastically less expensive and commonly available. Since all of the infrastructure concepts presuppose an edge device with a high assurance security kernel and added end-to-end Suite B encryption capabilities, the link layer encryption might prove of little value due to the increase in latency. The cost for these architectures is a function of the number of bases multiplied by the number of additional wireless sites required (existing access points are considered a sunk cost). Although difficult to enumerate without implementing scalable pilot programs, these architectures coupled with the MVNO concept can bring significant cost savings. As an example, T-Mobile offers cellular plans that provide unlimited VoIP minutes independent of customers' cellular minutes and at no additional cost to the customers.

c. Department of Defense Allocated Spectrum

The final option to consider when developing a communication plan is whether to use DoD-owned or allocated spectrum. For example, in some instances, the government spectrum might be the only authorized frequencies for military services. When deployed overseas, the available spectrum is allocated by the host country or other coalition partners. Domestically, if commercial signals are unavailable or unlicensed spectrum is too congested, the DoD spectrum remains the only feasible option. From the authors' personal experience, the military services' inherent wireless communications devices provide robust signals for the most extreme austere environments. These signals provide security properties that are not found in the commercial market (i.e., low probability of detection (LPD), low probability of intercept (LPI), low probability of exploitation (LPE), and antijamming (AJ)). Although some commercial signals inherently provide a limited level of these characteristics (i.e., CDMA), the signals were not intended for protecting against emission threats; rather, the commercial signals were

designed with these properties to increase connectivity performance (Dixon, 2010). Since the DoD spectrum is more widely available for military operations, and the military wireless communication networks are designed around these frequencies, it seems feasible to evaluate the cost of the spectrum and potential architectures that leverage this spectrum.

(1) *Spectrum Cost.* Given that spectrum is a finite resource and continually in high demand, some argue that the federal government should reallocate more spectrum for commercial purposes. This argument is hard to discount when looking at the resulting revenue from various actions. For example, the U.S. federal government received over \$19B from the 700MHz band and over \$13B from the Advanced Wireless Services (AWS) band actions—although reallocating this spectrum did cost the government in terms of labor and equipment to move or modify the systems (FCC 2009; FCC 2010). In some cases, the legacy equipment was obsolete and, therefore, newer equipment was easier to buy without major loss in capabilities. In other cases, the newer system was not feasible and, therefore, a loss in capability was inevitable. To mitigate a large detriment in capabilities, the reallocation period was extended over a couple of years, depending on the specific circumstances. Fortunately, for the affected government agencies, on December 23, 2004, President Bush signed the Commercial Spectrum Enhancement Act (CSEA) to provide assistance in recovering reallocation costs from auction proceeds (Office of Management and Budget, 2007). For the AWS band, the government allocated over \$1B of the revenue towards facilitating the reallocation of Federal communications systems (Office of Management and Budget, 2007). Of the \$1B in recovery cost, the DoD only received a proportion. Table 16 illustrates DoD allocations:

Departments	Amount	Timeline	Systems Affected
Air Force	\$106,753,481	48 Months	36
Army	\$15,933,043	36 Months	31
Navy	\$134,465,000	36 Months	29
DoD-wide support	\$98,200,000	72 Months	
Total	\$355,351,524		

Table 16. DoDs Plan for Spectrum Reallocations Funds

The licenses auctioned under the 700Mhz and AWS bands were issued for 10 to 15 years.¹¹³ Given the combined sum of about \$33B minus the few billion in reallocations cost, the federal government is still poised to realize an increase in at least \$2B per year across the next 15 years. Therefore, the argument against maintaining exclusivity of government spectrum is very difficult to justify. The CSEA has made the reallocation of spectrum a little less burdensome for the effected bureaus; however, these organizations never receive the full recoupment of cost. Although these two bands received a high return at auction, some spectrum is not valued as “prime real estate.” When evaluating future bands for reallocation, the business cases should ultimately look at the opportunity cost—how much is it costing the government to maintain exclusivity rights. Alternatively, as a representative from ASD NII stated, even though the government business case looks promising, the individual departments’ business cases fail to provide enough justification for releasing the spectrum. For example, using the AWS band, the DoD was allocated \$355M in return for their lost spectrum. When dividing that across 15 years, that returns \$24M per year. Those funds seem sufficient to cover the cost of modifying and procuring the equipment (i.e., 96 systems); however, they may not be sufficient for leasing back the spectrum when needed. As quoted from network operators, the cost to lease spectrum can range from hundreds of dollars per month to thousands, depending on the area. Given these price

¹¹³ Sourced from the FCC Fact Sheet. Retrieved from http://wireless.fcc.gov/auctions/default.htm?job=auction_factsheet&id=66.

points and assuming the DoD occupies at least 100 locations with underserved coverage, the cost to lease the spectrum to propagate cellular emissions (i.e., base stations) could range from hundreds of thousands to tens of millions.

(2) *Tethered*. The tethered concept leverages inherent IP-based military radios for all wireless transmissions.¹¹⁴ Assuming the approach in Chapter III exists (i.e., the smartphone devices already supports high assurance separation and virtualization as the architectural foundation for any guest operating systems), the level of modification required to implement the tethering concept is trivial and the cost is insignificant (Lyons, 2011). If the smartphones only contained the high-level operating system with an inherent unmodified kernel, this concept's TCO becomes cost prohibitive, fails to address various security vulnerabilities, and requires additional cabling. Figure 35 illustrates a simplistic view of the concept, but additional variations are feasible (i.e., vehicle mounted radio with dash mounted sled, etc.).



Figure 35. Tethered Smartphone to Military Radio

(3) *Tactical Waveform*. In environments that preclude commercial emissions due to threats of detection, interception, or exploitation, tactical signals continually prove adequate for mitigating the risk. However, those capabilities traditionally come with a loss of functionality. The tactical radio signals can provide the ability to increase emission security, but the radios' functional inefficiencies inhibit their ability to match the communication capabilities of commercial devices. In an effort to

¹¹⁴ Refer to Dixon (2010) and Lyons (2011) theses for more details surrounding the tethered concept.

provide both these capabilities, this paper suggests designing and manufacturing a small chipset with inherent tactical signals contained within current military radios. From a sleeve design, similar to common cases for almost every modern day smartphone (e.g., Figure 36), these chipsets and added battery power could provide the transport medium for smartphones. Essentially, a smartphone wrapped with these sleeves facilitates modern day innovative features while maintaining traditional emission securities. However, this approach assumes the handset leverages the high assurance separation architecture as mentioned in Chapter III.



Figure 36. Smartphone Sleeve Concept¹¹⁵

The cost to research and develop this specialized sleeve is difficult to estimate since very few publicly available efforts are known. Lockheed Martin has a program that attempts to use their proprietary base station and wireless protocol. Their sleeve and associated base station are not exactly the same as this concept, but at least are one step closer. Additionally, the device communicates between the smartphone and the sleeve via standard Wi-Fi protocol, whereas this concept should leverage tethered links via the USB or 30 pin connectors. The cost for Lockheed Martin's sleeve is around a thousand dollars. Mass quantities could drive the price lower. The difference in the concept presented here is that the sleeve connects directly with legacy radios vice a modified base station. Therefore, the cost of Lockheed Martin's base station is not a factor when considering similarities. Since this concept leverages preexisting waveforms, the typical tens of millions of dollars spent on protocol research and development would also not be a factor. However, the cost to consider here is the porting of the protocol (i.e., waveform) from the current form factor to a small chipset—additional costs to consider

¹¹⁵ Image retrieved from www.apple.com.

include: personnel, encryption (Type 1 vice Suite B), supply chain, maintenance and support, etc. The authors suggest a feasibility study be conducted for this approach—currently a significant number of unknown variables exist.

4. Commercial Grade Core Network Cost

This section captures the cost¹¹⁶ of procuring core network capabilities to host 2G/3G cellular services. The cost estimated in this section is based on the business case that is detailed in Addendum A. Additionally, previous Yuma proving grounds core network expenses were used as a comparison for estimating the cost to support millions of subscribers.¹¹⁷ Table 17 lists the aggregated services and their respective costs required to host a 2G/3G core network. These services can vary depending on requirements. This paper considers the base station controllers as an edge network component, and therefore those costs are not included in this section. However, there are a significant number of other potential costs (i.e., additional labor for maintenance and support, additional plant property and equipment [PP&E] to support extra equipment, etc.). The authors believe additional work is necessary to accurately depict all the associated cost; however, based on our knowledge, these estimates seem reasonable.

¹¹⁶ See Addendum A for previous business case analysis.

¹¹⁷ Referenced sources are labeled as government distribution only; however, the data presented in this section is distilled into a public released format.

Description	Quantity	Minimum	Maximum
Mobile Switching Center (incl. Visitor Location Register (VLR))	2	\$1,600,000	\$2,000,000
Media Gateway	2	\$400,000	\$600,000
ISDN user part (ISUP)/Session Initiation Protocol (SIP)	2	\$400,000	\$600,000
Home Location Register (HLR)/Authentication Center (AuC)	2	\$200,000	\$1,400,000
Short message service center (SMSC)	2	\$600,000	\$1,400,000
Voice-mail Server	2	\$800,000	\$1,000,000
Serving GPRS Support Node (SGSN)	2	\$200,000	\$1,000,000
Gateway GPRS Support Node (GGSN)	2	\$200,000	\$300,000
Operations & Maintenance (O&M) System	1	\$100,000	\$200,000
Total		\$4.5M	\$8.5M
Total per year (7 year lifetime)		\$640K	\$1.2M

Table 17. Potential Cellular Core Network Cost

C. BENEFIT

Since the purpose of the MVNO business case was to highlight solutions to reduce cost, increase security, and increase signal coverage, this section details the benefits within those categories.

1. Customer Service, Sales, and Billing

From the fifty-thousand-foot view, the benefit for in-housing the customer service, sales, and billing portion of wireless services is the reduced procurement cost and added security policy capabilities. As mentioned in the beginning of this chapter, the DoD spent roughly \$235M in FY2010 and continues an increasing trend of \$40M per year for cellular services. Over the next 5 years, given a constant discount rate of 3%, the net present value for the potential cost is about 1.475B. If the customer service category is adopted using the worst scenario from the cost section, the cost to the DoD is about \$577M. Therefore, the total realized saving from implementing this concept is about \$898M.

a. Telecommunication Expense Management

A Telecommunication Expense Management (TEM) solution provides services for sourcing, procurement, and auditing (Goodness & Redman 2010). These services provide the customers with data points for negotiating prices, contract terms and conditions, improved financial forecast, and usage planning (Goodness & Redman 2010). Additional services include ordering and provisioning, inventory, usage, and dispute management (Goodness & Redman 2010). Since these categories are a subset of the customer service, sales, and billing MVNO concept, the benefits of a TEM solution are very similar in comparison. Assuming that a significant part of the DoD already contracts TEM providers (i.e., multiple TEM providers are listed under the General Services Administration (GSA) contract site), then a portion of the benefit is representative of their cost. Searching the GSA website, the cost for these solutions resides in the vicinity of hundreds of thousands of dollars annually. The remaining benefit is representative of the wasted expenses from non-TEM participating departments. This could result in millions of dollars in annual savings by consolidating the various TEM providers into one DoD solution. Based on a market research report, the best-in-class commercial company is able to save 18% annually on wireless expenses by leveraging TEMs services. Assuming 25% of the DoD does not implement a TEM solution, then this would provide a benefit of \$49.5M for FY2011 (i.e., \$275M [projected FY2011 expenditures] x 18%). Although not included in many of the TEM solutions, some TEM providers are including increasingly valued over-the-air Mobile Device Management (MDM) solutions as a way to differentiate their product offerings (Goodness & Redman 2010). This capability provides real-time access and control of every mobile wireless device. Again, since this service is inherently available for MVNOs the benefit is difficult to enumerate.

b. Local Telecommunication Offices Capacity

Since a majority of base telecommunication offices support wireline and limited wireless services, their unused capacity may be considered sunk cost or opportunity cost. If this MVNO concept was implemented, these telecom offices represent a prime candidate for providing the base customer service offices. Since the DoD has wireline services, the organization is already structured to facilitate

communication like processes (e.g., DISA operates the defense switch network). Therefore, in some cases, and depending on capacity, the added wireless services might only require additional personnel instead of completely reorganizing the personnel, facilities, work processes, etc.

*c. **Reduced Contracting Costs***

Another benefit not thoroughly investigated in this paper is the reduction in contracting cost. Under this MVNO concept, the generation of tasking orders and delivery orders might be replaced with military interdepartmental purchase requests (MIPRs) or other interdepartmental funding processes. Since the actual purchases from commercial vendors are consolidated under a program office and procured in bulk orders, the individual commands can maximize opportunity cost by reallocating resources. For more insights into the actual cost savings, a further analysis through business process reengineering is suggested.

2. Integrated Voice-Mail and Messaging Services

Since this concept builds from the previous MVNO concept (i.e., customer service, sales, billing, etc.), the same benefits exist. However, a couple unique benefits to this concept exist as a result of inherently controlling the voice-mail and messaging services.

*a. **DoD SMS/MMS***

In disaster situations, where distributing recall messages or publicizing command-wide notices is extremely important, an automated initialization service vice a human-in-the-loop process potentially becomes a necessity. Assuming a majority of department personnel have mobile devices provisioned under this service or linked through a client application, this approach (i.e., sending instant notifications) seems feasible. For example, military commands develop threat levels with associated policies and procedures for instances of severe weather that could cause loss of life or equipment degradation. The ability to automate the delivery of these notifications can significantly enhance the response time. Continuing with this example, and leveraging the capabilities that this concept provides, the commander, department head, or delegated authority could

implement an instantaneous unit-wide notification directly to every handheld device. Additionally, these systems could facilitate automatic tallied responses for personnel accountability purposes. Essentially, as the storm rolls through the region, the leaders could send and receive real-time updates on threat levels and personnel readiness. The benefit received potentially equals the cost of a loss in life or equipment. Since the military has extremely high valued equipment (i.e., in the order of billions) this paper will only quantify the value of a life to evaluate an order of magnitude for benefits. Using the value of life equation cited in a previous cost benefit analysis, this paper defines the value as a function:¹¹⁸

$$V_L = \frac{\Delta E}{\Delta R} \left(\begin{array}{l} V_L = \text{Value of Life,} \\ \Delta E = \text{Marginal Change in Earnings, and} \\ \Delta R = \text{Marginal Change in Risk} \end{array} \right)$$

Figure 37. Value of Life Equation (From Lakamp, McCarthy 2003)

In Lakamp's (2003) thesis, the author's value of life was about \$3.7M per employee. Since they used military personnel and DoD civilian employees in calculating risk, the results are similar to this example. Additionally, their assumptions for employee earnings were roughly similar to this example.¹¹⁹ Assuming a more conservative value of life at \$3M per employee, the added benefit in this example results in \$3M times the number of potential deaths for any given disaster situation. As the number of potential deaths increases beyond 333 employees, the cost breaks the billion-dollar threshold. However, the likelihood of this number of casualties seems small. The referenced thesis used the Oklahoma City terrorist attack as a potential event, which resulted in 14% fatalities. Obviously, when evaluating the benefit received from a technology that could prevent loss of life, the return is high.

¹¹⁸ David Lakamp; Gill McCarthy. (2003, December). "A Cost-Benefit Analysis of Security at the Naval Postgraduate School." Monterey, CA.

¹¹⁹ The thesis valued \$55,890 as the average annual earnings.

b. Integrated Voice-Mail

Another benefit is the ability to consolidate all voice-mail services into one secure solution—a secure solution meaning inherently owning the management, operational, and technical policies governing the implementation.¹²⁰ For example, military personnel might have one or many phone numbers assigned to them as they progress through their career. This type of solution could enable a secure voice-mail service per employee, independent of their current phone number or attached command, that would travel with them as they move—similar to official e-mail accounts. Some benefits potentially received from this type of service are a reduction in vulnerability from the current system (i.e., assuming the current systems are vendor-provided solutions), an increase in usability (video voice-mail or voice-to-text voice-mail service, etc.), and the added convenience of a consolidated voice-mail rather than three separate voice-mails on three different networks.

3. Edge Network

Since this concept builds from the previous MVNO concepts (i.e., customer service, sales, billing, integrated VM, and messaging), the same benefits exist. However, a couple of unique benefits to this concept exist as a result of inherently controlling the edge network devices.

a. Mobile Intranet (Data Side)

If the DoD decides to procure edge network base stations and access points, the decision could provide the ability to connect via an intranet network. Essentially, the locally owned, controlled, and approved access points or base stations could provide the entry point for on-base intranet access. The ability to integrate the voice capability via standard cellular protocols would still require a core network. However, a secure VoIP architecture leveraging SCIP might provide an alternative

¹²⁰ Refer to Appendix A in regards to security definitions.

method for voice communications and on-base DISN access. Unless the phones were customized with an inherent SCIP capability, the devices would require a client application to participate in that network.

b. Increased Signal Coverage

As previously highlighted in Figure 30, the world still lacks ubiquitous commercially available cellular coverage. This MVNO concept provides the flexibility of adding additional edge network devices to connect CDS COTS smartphones. This could provide the military services with a marginal productivity increase for operational deployments that lack commercial signals (i.e., resulting capability from adding the data functionality to a traditional voice only network). For example, in areas that lack sufficient commercial signals, the military services could erect edge network equipment to support the mission throughout the duration of an exercise. Alternatively, on domestic military bases with limited cellular coverage this MVNO concept provides the ability to add the coverage based on military priorities vice commercial market demand.

c. Added Competency for Operational Deployments

Another advantage of owning the edge network devices is the ability to grow inherent competency surrounding the base station technology. As the use of this technology increases, the operators and maintainers of the equipment will develop a greater understanding of commercial systems. This knowledge could provide a solution for military operations that require interoperable commercial communications with the local populace or coalition forces.

4. Commercial Grade Core Network

a. Mobile Intranet (Completely DoD-Owned Network)

This paper presents only a few potential benefits from adopting an MVNO approach, because a comprehensive perspective seems difficult to quantify with any degree of accuracy. One could postulate that the benefits received from typical enterprise architectures exist in the MVNO model. In Figure 38, the top block represents a typical model a residential customer could implement with service from a commercial network

operator. The middle block represents the architecture that same residential customer and every other mobile subscriber shares when leveraging mobile services. Alternatively, for the higher end customer (i.e., large organizations), the lower architecture is a potential architecture to provide additional security protections.

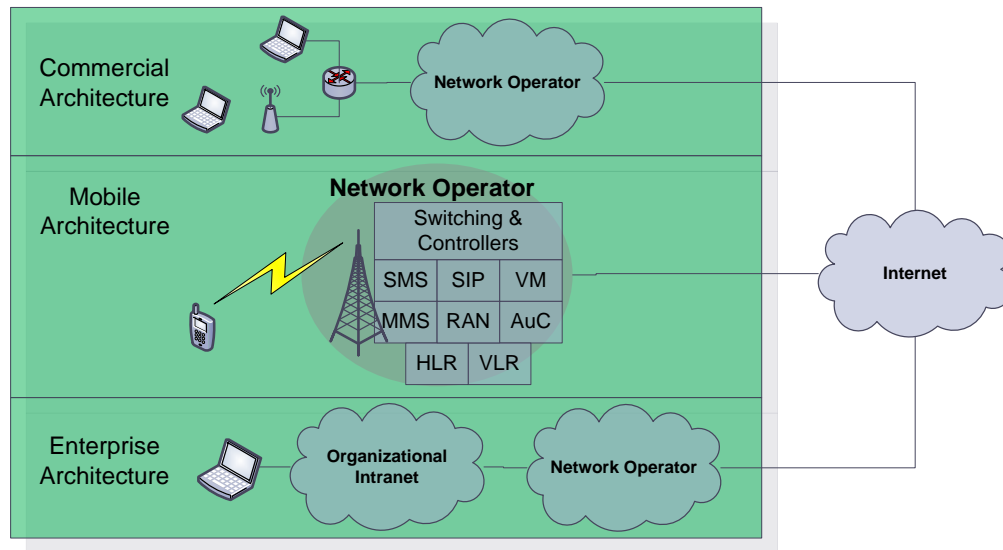


Figure 38. Network Architectures

In essence, these three models reflect basic mechanisms for connecting services through the Internet. Arguably, the enterprise architecture includes a protection layer that the other blocks are missing, including such additional services as firewalls, demilitarized zones, storage and power redundancy, network management suites, etc. If the DoD adopted the MVNO model, these different types of intranet services become a reality. Internalizing MVNO services can facilitate a separation or buffer between the end-subscriber and the external networks; otherwise, since the network operators own and control the radio access and core networks, the handset devices end up directly attaching without a mediator. As mentioned in the SME PED architecture, the MCEP middleware functions as a mediator. There are services unique to smartphones on which other computing devices are not typically dependent (i.e., SMS, MMS, Voice-mail, HLR, VLR, etc.), but these services are essential to provide the complete functionality of traditional services. Since these services exist, the MVNO becomes a desirable model to

leverage a more secure implementation. Since this model positions the DoD to procure the minutes and data rates at wholesale prices (i.e., in bulk), the organization can finally leverage economies of scale.

5. General MVNO Benefits

The following paragraphs provide various benefits shared across all the MVNO approaches.

a. Realigning Incentives

Currently, the DoD contracts and agreements facilitate pool options (i.e., monthly shared minutes, SMS, data, etc.) by tasking order to help reduce overage fees; however, the underutilizing user ends up bearing the cost of those unused minutes. The users who exceed their “allotted” minutes receive the additional minutes at the expense of the other users. For example, users 1 and 2 share a 500-minute pooled plan for \$60 per month. User 1 uses 400 minutes, and user 2 uses 600 minutes. In this example, no overages were charged, but user 1 pays 15 cents per minute (i.e., \$60/400 minutes) and user 2 pays \$0.10 per minute (i.e., \$60/600 minutes) even though they both contributed \$60 each to the pooled plan. Assuming the combined users do not consume beyond the pooled limit, this model does not incentivize the user to control over usage. Under the MVNO model, the organization can buy the service (i.e., minutes, text, data, etc.) in bulk and still distribute the minutes to their customers under a pay-as-you-go model. In this model, the cost burden is correctly aligned with the usage.

b. Specialized Handsets

As previously mentioned in Chapter III, a common method for the MVNOs to add value is to provide specialized handsets to their niche markets. In the DoD’s case, this is extremely valuable for each of the services (e.g., the Army and Marine Corps) who have their own operational requirements for smartphone-like capabilities. Each of the MVNO concepts facilitates the adoption of SIM branding and MVNO unique handsets.

c. DoD App Store

As previously mentioned, the iPhone jail breaking concept illustrates a vulnerability that is potentially mitigated via a CDS architecture implemented on a smartphone device. Assuming a CDS provides adequate protection against the vulnerability of flaws in manufacturer's installed software (i.e., providing unauthorized root access), this MVNO concept could facilitate additional security controls for safeguarding against malicious applications. If the DoD implemented an application store functionality (i.e., according to the Army, they are already starting the beginning of an Army app store), then perhaps third-party applications could enter the devices after qualifying the application for DoD use. This MVNO concept could provide the ability to "lock" the phones from installing third-party applications. The development of an app store in conjunction with implementing the MVNO concept provides the ability to implement a policy for authenticating applications, validating application integrity, and facilitating application authenticity.

d. Additional Security

The aforementioned network architectures can provide on-base (i.e., military bases) access through the properties required to reduce risk (i.e., increase security). The action of owning the equipment and therefore the security policies of the edge network provides an advantage depending on the environment. Each of the edge network concepts provides advantages such as spectrum agility, reduced cost, greater interoperability, and reduced threat. Note that some of the potential threats are not preventable through simply owning the edge network device.

D. RISK

In evaluating IT risk, the authors use the same risk equation presented in Appendix A (i.e., $\text{Risk} = \text{Vulnerability} \times \text{Threat} \times \text{Impact}$) as a guide. Ideally, an in-depth study of the specific threats, vulnerabilities, and impacts of specific architectures would yield the most granular comparison of options; however, this study only seeks to evaluate the potential for each implementation to reduce the IT risk below the risk level of the base case.

This section presents an evaluation of the potential for each MVNO network approach to reduce the opportunity of threat actions to exploit vulnerabilities—evaluation of threat and vulnerability occurred simultaneously. The authors performed this evaluation on the following threat actions that contained the highest combined potential: backdoor, electronic tracking, interception, masquerade, and intrusion. These threat actions contribute most significantly to the most pernicious threats, and they enable opportunities to enact other threat actions. For example, the existence of a backdoor may facilitate any combination of the following threats: exposure, falsification, corruption, obstruction, misappropriation, and misuse.

1. Residual Vulnerabilities

The definitions of the selected threat actions, as provided in Appendix A, follow:

- Backdoor: resident malware offers functionality allowing an attacker to gain access at will
- Electronic tracking: pinpointing a user’s location via his handset
- Interception: An unauthorized entity directly accesses data transiting between authorized sources and destinations. Examples include theft, wiretapping, and emanations analysis
- Masquerade: an unauthorized entity poses as an authorized entity to gain access to a system or performs a malicious act. Examples: masquerading via spoofing or malicious logic, system cloning
- Intrusion: an unauthorized entity bypasses or subverts authentication mechanisms to access sensitive data. Examples include trespassing, system penetration, cryptanalysis, and social engineering

Table 18 shows the interpretation of the authors’ evaluation of each network’s potential vulnerability, given the listed threat actions. The numbers 0, 1, and 2 represent high, medium, and low residual vulnerability, respectively. The left two columns (i.e., highlighted with light grey) represent the current approaches authorized to transport unclassified and classified information, respectively; the middle columns represent the

MVNO approaches, and the far right columns (i.e., dark gray) represent additional edge network approaches. The ensuing paragraphs describe the evaluation methodology.

Approaches	Current		MVNO					Edge Network Access				
	Commercial MNO (Retail)	Commercial MNO w/ MCEP	Customer Service, Sales, Billing	Integrated VM and Messaging	Edge Network w/ Commercial Core	Core Network w/ Edge Network	DoD MNO	Mobile Base Station	Enhanced WiFi (Garrison)	Enhanced WiFi (Tactical)	Tethered Tactical Networks	Tactical Waveform Sleeve
Residual Vulnerabilities												
Backdoor	0	2	2	2	2	2	2	0	2	2	2	2
Electronic Tracking	0	0	0	0	1	1	1	1	1	1	2	2
Interception	0	2	2	2	2	2	2	1	1	1	2	2
Masquerade	0	1	1	1	1	1	1	0	0	0	2	2
Intrusion	0	2	2	2	2	2	2	1	1	1	2	2
Score	100%	30%	30%	30%	20%	20%	20%	70%	50%	50%	0%	0%

Table 18. Residual Vulnerabilities (Network Vulnerability Given Threat Action)

In Table 18, the current commercial and SME PED approach (light grey columns) provides the “AS IS” model. The MCEP essentially provides a secure tunnel for connectivity between the SME PEDs and higher domains. By the nature of its design, and assuming its proper implementation, the architecture mitigates a significant number of threats. Over the commercial mobile architecture, the MCEP protects against the selected threats in the following ways: backdoors via physically separated domains; interception via HAIPE protected tunnel. The commercial MNO approach results in the highest residual vulnerability, because the network implements less desirable management, operational, and technical security controls.

In Table 18, the middle columns leverage the same MCEP architecture and, therefore, are afforded the same level of protection. However, since the MVNO approaches integrate edge and core networks inside base perimeters, the threats are

potentially limited to the base. For example, positioning the base stations inside military bases perimeters reduces the threat of RF detection, because personnel access to base is limited to authorized personnel.

Finally, the military network extension approaches (i.e., tethered and sleeve) appear to have the lowest risk. Assuming these extensions provide the same level of protections as the connecting networks, these approaches inherently offer additional flexibility. For example, natural and environmental threats are mitigated by the components being ruggedized and portable. The RF properties (e.g., low probability of detection, interception, exploitation, and antijamming) of the tactical waveforms provide mitigation characteristics to limit signal interception, masquerade, electronic tracking, and obstruction. Since the approach does not include network management tools for implementing controls against falsification, authorized parties could subvert the system. However, the threat is reduced if the system leveraged the MVNO approaches. The likelihood of corruption, misappropriation, and misuse is reduced, assuming that the military tactical networks are configured manually vice over-the-air (OTA), and the previously mentioned mitigations exist. Refer to Appendix I for a more thorough discussion surrounding threat action and security controls.

Figure 39 highlights the same information as Table 18; however, this figure provides a better visual comparison of the various approaches. The mobile base station approach results in a higher residual vulnerability, because the various vendor solutions use the same commercial protocols used in the commercial MNO. Additionally, independent of other services, they still lack the network management characteristics (i.e., telecommunication expense management, mobile device management, etc.). The resultant score is less than the current commercial implementation, mostly because the management and operational policies are controlled by the owning organization.

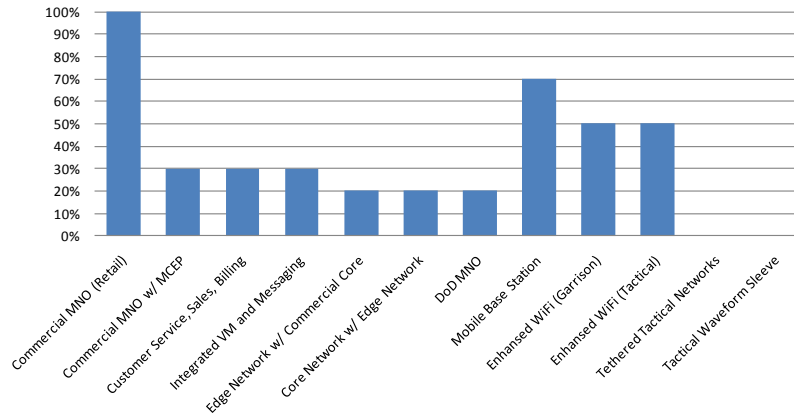


Figure 39. Residual Vulnerabilities Graph

2. Value of Information (Impact)

Impact represents an important component of the risk equation. This paper assumes the marginal risk (i.e., difference between the current risk and the risk remaining after implementing a new architecture) represents a benefit to the system. In order to quantify risk, the authors assume the value of information is a function of the potential for degradation to the U.S. gross domestic product (GDP). Since the various levels of classification (i.e., confidential, secret, and top secret) are categorized depending on the potential to cause damage, serious damage, and exceptionally grave damage to national security, respectively, the authors assume the value of that type of information is directly correlated to the value of national security.¹²¹ Assuming the United States values its national security higher than the cost to operate and maintain the DoD, the value of national security is at least the cost to operate and maintain the DoD. According to the FY2012 budget, the DoD was allocated about \$700B in FY2010; and according to the U.S. Bureau of Economic Analysis (BEA), the U.S. GDP was about \$14.6T for 2010. Therefore, the authors assume that the U.S. valued its national security at 5% of the GDP in FY2010. Based on these ratios, the authors assume the value of information is as delineated in Table 19. Although the defining characteristics categorizing these levels of

¹²¹ Reference Federal Register, Vol. 75, No. 2, for more details about the current policy in regards to these categories.

classification are ambiguous, the ratios found in Table 19 seem representative of the minimum values (e.g., the characteristic “exceptionally grave damage” seems at least equal to 0.068% of a country’s annual income).

Levels of classification	Cost (ratio of 2010 GDP)
Unclassified	Cost of components
Sensitive but unclassified	Hundreds of Thousands
Confidential	Tens of Millions (0.000068%)
Secret	Billions (0.0068%)
Top Secret	Tens of Billions (0.068%)

Table 19. Value of Information (Impact)

3. Risk Calculation

Combining the percentages in Figure 39 with the cost of the various levels of classifications in Table 19, the authors quantified the value of risk associated with each MVNO approach. The marginal risk is equal to the difference between the current risk (i.e., commercial cellular service + secure service) and the proposed risk.¹²² After application of this methodology, Figure 40 represents the overall risk associated with each domain. The data point for each approach is the proportion of risk (percentage) to the overall risk for each domain. This figure illustrates the distribution of risk for each approach across the domains. The current SME PED approach results in a higher risk for the domains containing information of low value because the cost of the device outweighs the cost of the information. However, as the value of information increases, the cost of the devices begins to marginalize—i.e., the high value of information overshadows any fixed-price unit cost. The lowest resulting risk is achieved if the DoD owns the core network.

¹²² Current threat and vulnerabilities is illustrated in Figure 40.

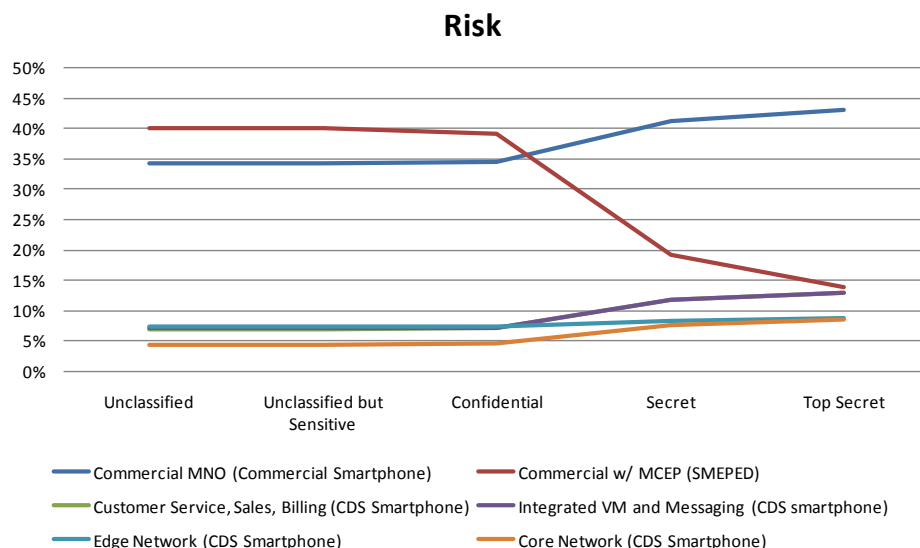


Figure 40. Percentage of Risk for Each MVNO Approach

E. SENSITIVITY ANALYSIS

Based on a number of variations in the previous models, it appears that hosting a dedicated network to support classified traffic seems infeasible. First, the lower demand will not provide enough volume to justify wholesale pricing with the commercial carriers. Second, the cost to procure a core network, including the RAN, and backhaul operational leasing expenses create a large fixed cost. Even if the cost is amortized over 7 years (equipment lifetime), the dedicated network is still cost prohibitive. However, if volume increases or the cost of the network is shared with the unclassified DoD cellular procurement demand, then the business case might become justified.

Figure 41 represents the potential cost to the DoD if the MVNO approaches were implemented at various levels of demand. The figure highlights approaches with relatively low overall cost and low demand, except for the MNO approach. The MNO approach assumes the DoD owns the mobile spectrum rather than leasing the spectrum from the carriers. The cost to own the spectrum is derived from the previously mentioned 700MHz and 1710MHz FCC auction examples (i.e., \$6B–\$9B per carrier for large quantities of spectrum amortized over 10–15 years). This approach was not mentioned as

a likely candidate, because the cost for owning the spectrum—in either opportunity cost or actual licensing cost—is expensive unless a subscriber base is present.¹²³

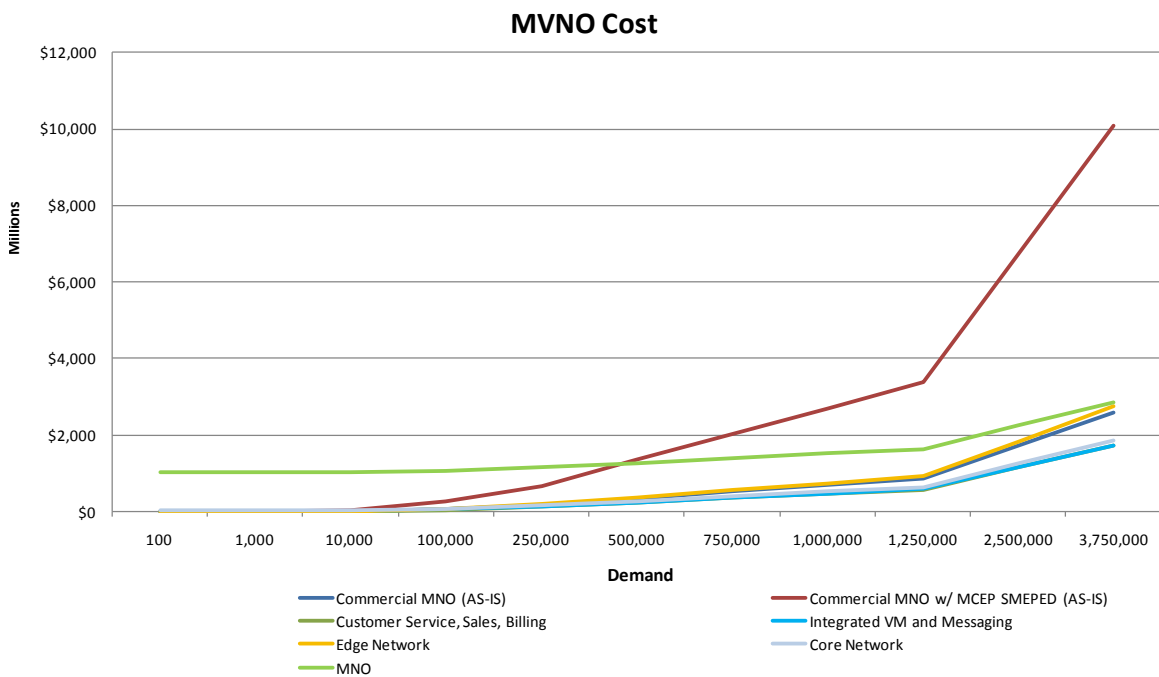


Figure 41. Cost of MVNO Concepts

In Figure 41, the “commercial MNO” line represents the cost associated with the current commercial network that the DoD uses to connect their smartphones to the DISN enterprise services. Notice that as the subscriber base for the MCEP architecture with associated SME PEDs increases, the approach becomes cost prohibitive.

The high unit cost of the SME PED results in a steeper cost curve. However, assuming a higher demand correlates to a high number of purchased units, the authors assume this translates to an increase in manufacturer efficiencies, which, in turn, reduces the device unit cost. However, in low quantities, the SME PED approach (i.e., including handsets) is representative of the trend highlighted in the left graph of Figure 42. The drastic increase (i.e., at quantity 1000) in the SME PED cost is driven by the cost of the handset. The right graph in Figure 42 illustrates the approach without including the cost

¹²³ Refer to Figure 42 for further discussion.

of the SME PEDs. Notice the lowest cost approach in Figure 42 is the one where the services are purchased directly from the carriers (i.e., commercial MNO).

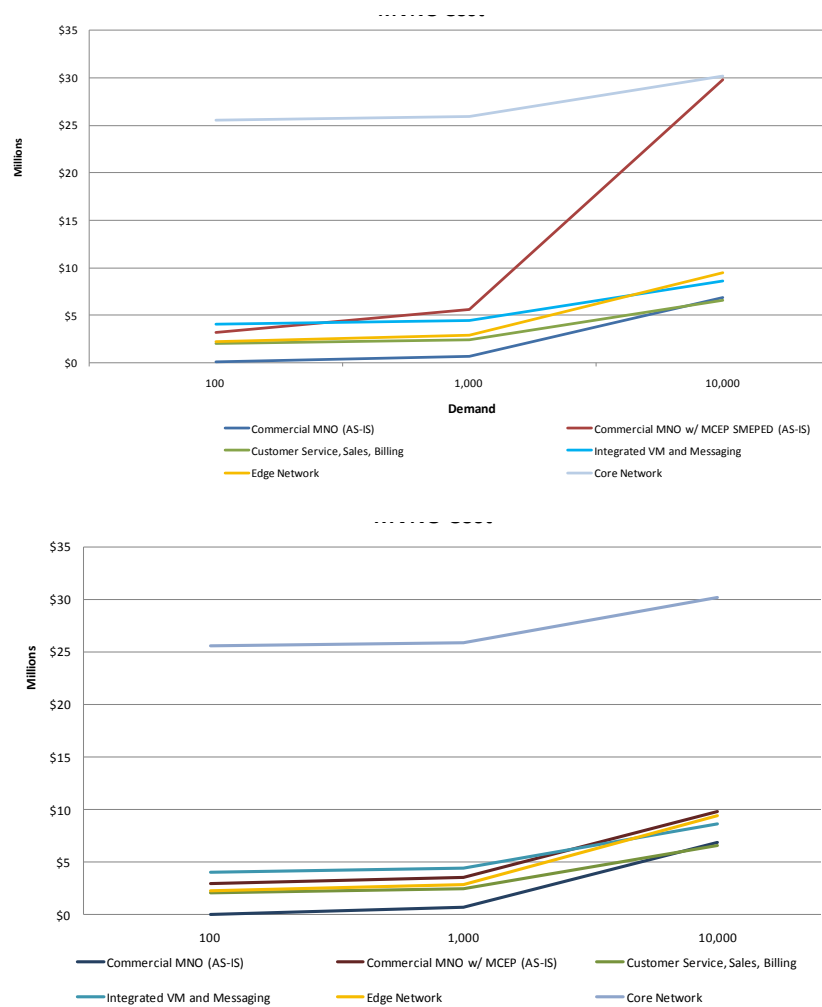


Figure 42. Cost of MVNO Concepts at Lower Levels of Demand¹²⁴

Assuming the cost of the SME PEDs will decrease at higher volumes, although the current fixed price contract might limit short-term cost reduction, Figure 43 illustrates the estimated trends based on SME PEDs leveraging economies of scale. Another important point illustrated in Figure 43 is the tipping point when the higher subscriber base starts to favor the core network approach. This is a result of the higher demand offsetting the high fixed cost of procuring the equipment. In this figure, the core network

¹²⁴ Figure 42 is illustrated only to show how unsustainable the SME PED approach is for higher demands.

approach follows the trend of the other MVNO approaches. This is a result of the cost for intercarrier roaming. The authors assume the core network approach can reduce commercial MNO dependencies. However, given that DoD personnel would need to roam on the MNO networks (e.g., intercarrier roaming) outside of organizational boundaries, the authors assume 50% of the current usage will continue as roaming.

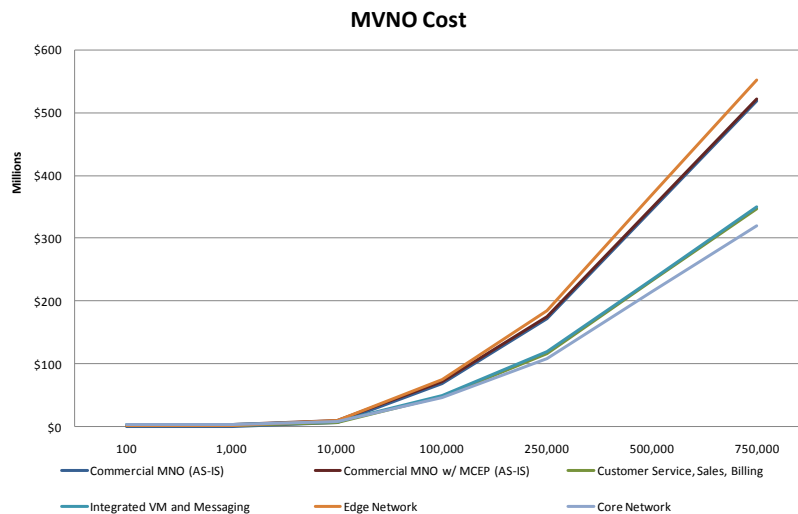


Figure 43. Cost of MVNO Concepts at Higher Levels of Demand

Based on the business case from Network Strategy Partners (2009), the carriers pay a significant amount of their operational expenses for interconnecting lease lines. Since the DoD already provides internal wireline services (i.e., Defense Switched Network), perhaps the cost of interconnecting the bases for ubiquitous wireless services can offset or even eliminate the cost by leveraging additional capacity. Figure 44 illustrates the MVNO cost without including the cost for the interconnecting lease lines. Notice the MNO approach becomes more desirable around the 3.5M subscriber level. Additionally, if the DoD owned the interconnecting lines rather than leasing them, the trends would look similar. An additional point of interest in this figure is the tipping point where the core network approach becomes the least costly (i.e., where the size of the subscriber base is about the same as the current DoD demand for unclassified wireless services).

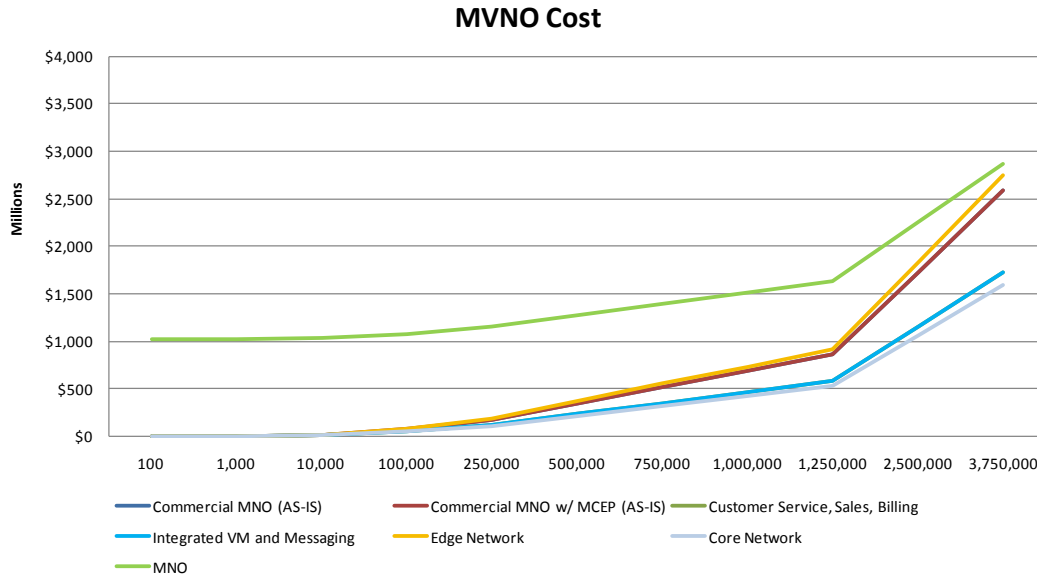


Figure 44. Cost of MVNO Concepts (Risk and Lease Line Expense Not Included)

Based on the MVNO concepts and the DoD's current demand, Figure 45 represents a more accurate estimate of what the DoD could expect to pay as demand increases. Again, these costs represent a very conservative view. The DoD's actual costs are more likely to show a more significant margin between the commercial and the proposed MNVO approaches. The cost of the edge network is consistently greater than the commercial option, because the cost of the edge network devices and the cost to lease the spectrum do not offset any other cost. As illustrated in Figure 45, as the demand increases, the marginal cost between the reseller approaches and the core network approach increases. This is a result of the high fixed cost for the equipment and the low reoccurring operating cost.

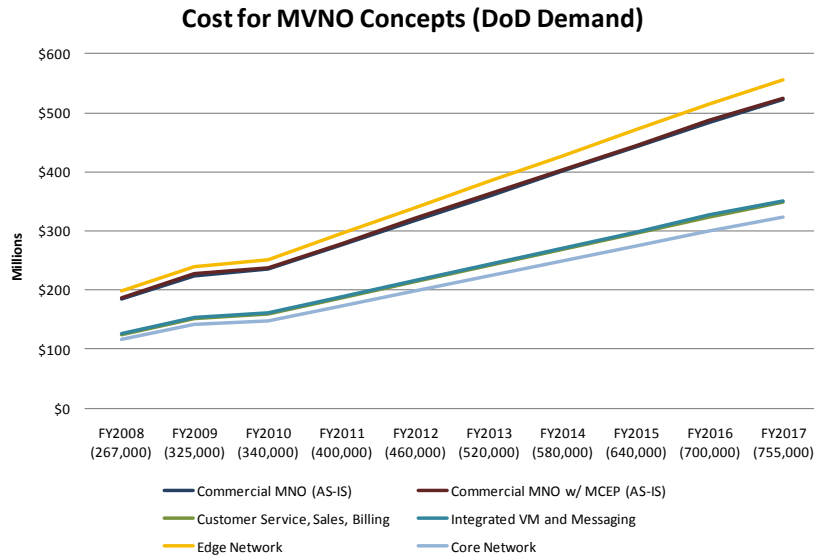


Figure 45. Cost of MVNO Concepts (DoD Forecasted Demand)

Figure 46 represents the monthly cost per user for each approach. Based on the previous costs, Figure 46 divided the cost by the number of subscribers to highlight a per-user cost. The most important result is the \$20 savings per user per month related to the current model. As previously mentioned, marketing costs represent the cost driver in the MNO market (i.e., 40–60%). The potential savings shown in Figure 46 seem consistent with the cost for marketing. The MVNO core network concept includes the cost of owning additional base stations and leasing spectrum. These MNVO approaches provide a mechanism to increase coverage, increase security controls, and ultimately reduce cost.

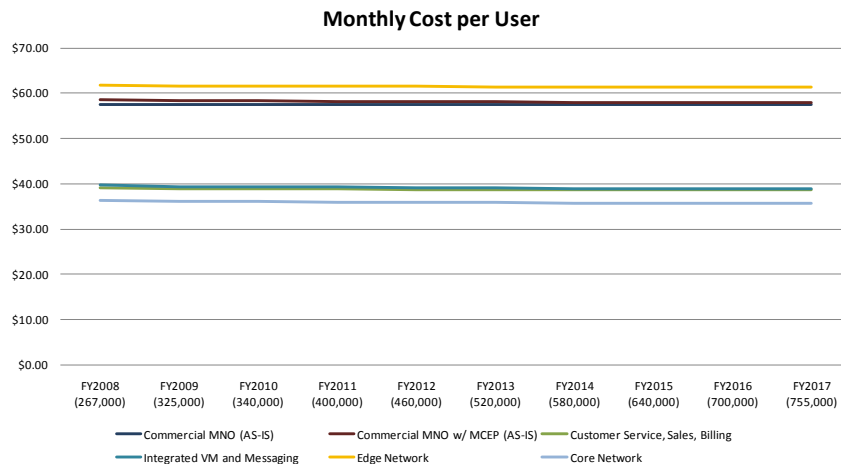


Figure 46. Monthly Cost per User for Each MVNO Concept

THIS PAGE INTENTIONALLY LEFT BLANK

V. COMBINED BUSINESS CASE AND CONCLUSIONS

This chapter summarizes the major results from the analyses that were performed in this project. The goal of the analyses was to identify strategies and business cases to support reduced costs, increased functionality, and the same or greater level of security for mobile communications in the DoD.

A. COMBINED BUSINESS CASE

Throughout the paper, the authors present multiple business cases to show the significance of adopting the MVNO model. Each of the business cases presents cost information, but so far the paper has not applied cost, risk, and benefit across the networks including the attached handsets.

Using this methodology and the data points from the previous chapters, Figure 47 provides a visual mechanism to evaluate the greatest potential for benefit—the lower the percentage (i.e., the lower the bar), the greater the benefits outweigh the cost. Figure 47 shows the cost of each approach, including the cost of the associated handsets, given a 300K subscriber demand. Each of the classification categories (i.e., unclassified, sensitive but unclassified, confidential, secret, and top secret) represents a specific domain containing the respective types of information. For example, the commercial MNO column over the unclassified category represents a commercial network hosting unclassified information. The associated value (i.e., 92%) represents the ratio of costs to benefits. An important note to consider is the cost for the commercial with MCEP approach. This figure was created with 300K subscribers; the price per unit might significantly reduce if the SME PEDs received that level of demand. However, the cost might not decrease significantly because the demand still lacks commensurate volume of the commercial market. The commercial with MCEP approach is not beneficial at higher volumes because of the high per-unit cost; however, as the domains increase in value (i.e., they contain higher valued information) the concept becomes more desirable. Notice in the unclassified, sensitive but unclassified, and confidential domains, the customer service, sales, and billing concept proves the most beneficial given the lower cost and less

risk. As the value of information increases, the core network approach becomes most desirable because it offers the greatest opportunity for employing operational, management, and technical controls of the network.

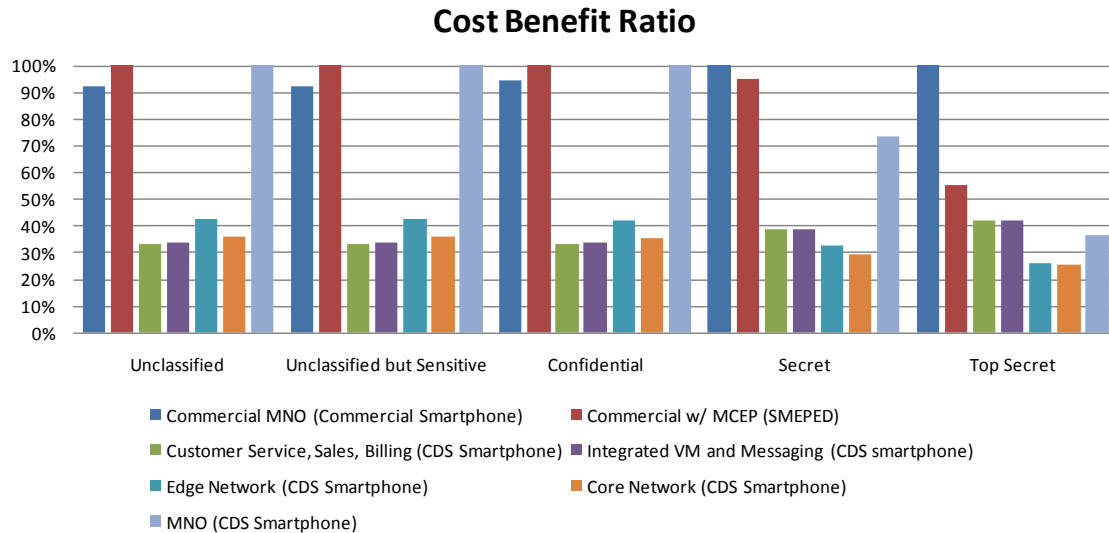


Figure 47. Cost Benefit Ratio per MNVO Concept (300K Demand)

Figure 48 represents the cost per user of each evaluated option. The commercial MNO approach with MCEP and SMEPED serves as the benchmark (illustrated in green), with costs accounting for 400K FY2011 projected subscribers for the unclassified domains and 2K SME PED subscribers. Since the subscriber base is large enough, the core network approach is the most advantageous.

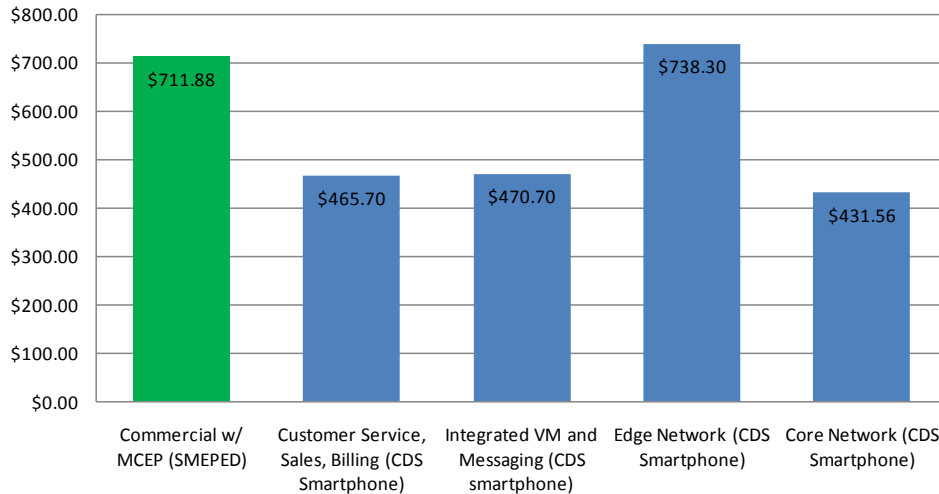


Figure 48. Cost per User for Each MVNO Approach

Figure 49 displays the cost per user for each of the additional network access approaches. These access points are considered as optional extensions depending on the current environment. Since these access points are considered optional, the total cost for the network devices are not included in the MNVO approaches. For example, the mobile base stations are potentially desirable for disaster relief operations; however, a fixed garrison environment might not be justifiable given the high cost per user. These costs are independent of the quantity because, as the users increase, the amount of required access points—to support the added users—increase in parallel.

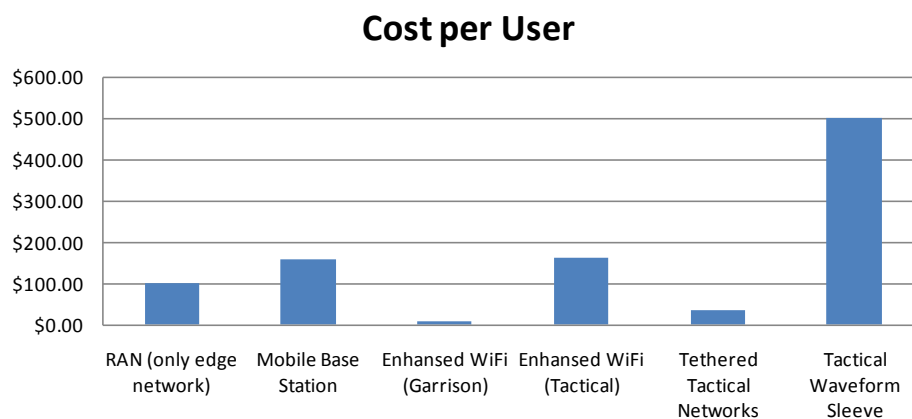


Figure 49. Cost per User for Each Type of Access Point

The per-user costs listed in Figure 49 illustrate a trend of increasing cost for devices that assist in decreasing the system-wide risk. For example, compare the commercial RAN network to the tactical mobile base stations, or compare the garrison enhanced Wi-Fi to tactical enhanced Wi-Fi. The difference in cost of the tethered and the wireless sleeve approach is a result of the increase in mobility, which requires additional complexity. Ultimately, the sleeve concept costs more per user than the other tactical access points; however, the concept provides a significant amount of risk reduction and an increase in mobility over the tethered architecture. The high cost for each sleeve is expected to decrease significantly, as the technology reaches the tail of its learning curve. These costs are only considering the annually reoccurring costs.

B. CDS SMARTPHONES

Based on the analysis performed in this project, staying the current course with the SME PED approach is more costly in comparison with various alternatives. The alternatives mentioned in Chapter III were to acquire CDS smartphones based on a high-assurance secure virtualization architecture, either via the federal acquisition procurement process or through a manufacturer that has integrated this technology into a product line architecture. The federal procurement option facilitates a greater control of requirements, but the manufacturer option increases the potential to leverage commercial economies of scale and decrease procurement times. Ultimately, a reduction in cost can assist in removing the self-imposed demand restrictions within the DoD. The following list contains some of the advantages to adopting a CDS smartphone that were identified through this research:

R&D Cost

SME PED (R&D) → \$44M (government cost)

COTS CDS (R&D) → \$10M

Unit Cost

SME PED (Procurement) → \$3675 (Amortized 2 years' lifetime)

COTS CDS (Procurement) → \$185 (Amortized 2 years' lifetime)

The SME PEDs cost the DoD a significant amount in opportunity cost. Given the current demand of 2,000 subscribers (i.e., with policy constraining demand) and an average 60 minutes of productivity increase from leveraging smartphones to minimize downtime in schedule gaps, we estimate the DoD could recover \$100–\$300M in annual productivity increases by switching to a COTS solution. The majority of the productivity increases are directly correlated to the increase in demand.

C. MVNO AS A SERVICE

Staying the current course with commercial retail wireless service cost the DoD \$235M in FY2010 and an additional estimated \$40M per year in each of the following years. The MNVO approaches in the worst case showed at least a 25% cost reduction (i.e., switching to an MVNO solution would save the DoD \$110M annually with an increasing savings trend of \$16M for each following year), compared to the current arrangements. The following table represents the AS-IS cost for the DoD to procure cellular services for unclassified and classified domains.

Current (AS-IS) Expenditures (7 Year NPV)

Commercial MNO w/ MCEP (SME PED)	➔	\$2.9B
----------------------------------	---	--------

Proposed MVNO (7 Year NPV)

Customer Service, Sales, Billing MVNO	➔	\$1.9B
Integrated VM and Messaging	➔	\$1.9B
Edge Network	➔	\$3.0B
Core Network	➔	\$1.7B

Given that the current monthly cost is estimated at \$60 per month per user, the MVNO cost per user resulted in a cost of \$40 per month. This cost is conservatively calculated because more savings are possible if the approaches are able to leverage sunk costs. This point applies if, for example, either the inter-base copper and fiber lines have additional capacity to support mobile users' traffic or the reduction in wireline traffic frees up capacity. This additional capacity could reduce the requirement for leasing lines

between bases. The current strategy is costing the DoD not only real dollars, but limiting the capabilities of the warfighters to leverage the services while deployed. The lack of available cellular signals in military training areas and operational environments precludes the organizations from leveraging this innovative technology. However, if the organizational structure is already built around an MVNO approach, the deploying commands could receive the services at their edges.

D. SUMMARY OF STRATEGIC OPTIONS

Both the MNO and handset manufacturer markets exhibit trends that indicate impending market saturation and increasing competition. The tenets of Porter's five forces state that these trends indicate decreasing bargaining power for those types of firms (Porter, 2008). This situation provides the following opportunities for the DoD to implement strategies supporting the aforementioned goals:

- Leverage the growing potential for secondary markets by implementing an MVNO business model while taking care to avoid the perception of competing with industry.
- Take advantage of handset manufacturers' reduced bargaining power to encourage development of features that the DoD values.
- Seek partnerships with entities that have similar values in order to increase bargaining power and influence development and offering of valued features.
- Contribute to education and increased awareness of security risks for both consumers and suppliers in order to speed the reduction of the gap between DoD and commercial demand for security features.

E. FUTURE WORK

Throughout the performance of this research, the following activities were assessed as lying beyond the scope, and therefore identified as future work:

1. Stratification of Values and Requirements of User Groups

An in-depth examination of the values of the commercial mobile user groups (e.g., residential, corporate, municipal government, etc.) should be conducted to provide the basis for determination of each group's mobile computing requirements. Knowledge of these requirements may then allow more precise identification of the overlap between DoD and commercial requirements. This information may contribute toward future DoD strategy development.

2. Detailed Risk, Vulnerability, and Threat Analyses of Specific Proposed Architectures

The risk assessment conducted herein only illuminates the potential vulnerability of each notional approach in the context of the evaluated threat actions. It provides an estimate of network risk, but contains wide variability depending on network architecture, variations in command policies, and differing operational standards. Therefore, it does not apply uniformly to all commands within the DoD; however, NIST (2002) states that a risk assessment should be tailored to the specific organization. By extension, the assessment should also ideally pertain to an existing or proposed architecture. To this end, the proposed future work may include determination of suitable architectures to implement the most favorable business case, and then perform detailed threat and vulnerability assessments in order to determine the risk to the DoD at a more granular level. Appendix I discusses a possible approach based on the assessment presented in Chapter IV.

3. Competency Requirement

Work may be undertaken to identify the competencies the DoD must develop in order to implement the business cases analyzed in this paper. An assessment of required competencies will assist in determining the viability of successfully executing the smartphone options examined in this paper.

4. Determine the Best Contracting Mechanism for Obtaining Wireless Devices and Services

This paper does not focus on the performance of the contracting mechanisms. More research is needed to evaluate the correct procurement process for DoD wireless services.

5. Determination of DoD Wireless Use by Region

The demand percentages in Appendix G are illustrated by region based on the physical locations of the funding offices. In some cases, the illustration might be misleading because the subscribers continually travel and rarely remain stationary in one region. Therefore, the authors recommend completion of a more thorough study to determine a more accurate representation of wireless usage by region. The accuracy of that study could drastically reduce the variability of the projections.

6. Quantify the Benefits of a Larger Feature Set

What are the benefits to the DoD of obtaining a larger feature set? For example, the SME PEDs are arguably years behind COTS smartphone innovations in features. What is the cost for the lack of modern applications or the ability for Soldiers, Marines, Sailors, and Airmen to develop in-house applications to increase productivity or refine business processes?

7. Cost of Spectrum

When evaluating future bands for reallocation, the business cases should ultimately look at the opportunity cost—how much is it costing the government to maintain exclusivity rights? What regulations or laws need to be enacted to protect the current federal spectrum holder or to reimburse the losing organizations for their loss of spectrum? These losses manifest as opportunity costs vice reallocation costs. For example, if the spectrum was auctioned for billions of dollars, the losing command should receive a significant amount of that money.

APPENDIX A. RISK, THREAT, AND VULNERABILITY

The purpose of this appendix is to summarize the definition of risk and present a risk evaluation methodology. The threats and vulnerabilities listed below should be considered when addressing system protection. They are applicable in the assessment of the overall risk to the mobile computing business cases proposed in this paper.

A. RISK

The National Institute of Standards and Technology (NIST) defined risk to information technology (IT) systems as “a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization” (NIST, 2002, p. 8). The risk determination methodology involves evaluating threat and vulnerability to determine a likelihood of occurrence, then multiplying this probability by the impact of successful exploitation; furthermore, this process involves the determination of security controls to minimize or eliminate the likelihood of exploitation (NIST, 2002). Although NIST describes a qualitative process for determining likelihood, the following equation depicts the relationships between the elements of risk: $\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact}$. The definitions of threat, vulnerability, and impact follow (NIST, 2002):

- Threat: The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability
 - Threat-source: Either (1) intent and method of enacting intentional exploitation of a vulnerability or (2) a situation and method that may unintentionally trigger a vulnerability.
 - Threat action: The method by which a threat-source executes an attack.
- Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and

result in a security breach or a violation of the system's security policy.

- Impact: The estimated quantitative or qualitative value of a loss or degradation of any combination of confidentiality, integrity, and availability.

1. Threat Actions

The following list provides a description of selected threat actions pertaining to mobile communications and IT systems and networks:¹²⁵

- Natural threat actions: For example, "Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events" (NIST, 2002).
- Environmental threat actions: For example, "long-term power failure, pollution, chemicals, liquid leakage" (NIST, 2002).
- Service abuse: malware or malicious users perform actions that cause higher than expected service provider costs.
- Backdoor: resident malware, possibly organic to the system, offers functionality allowing an attacker to gain access at will.
- Spam: unwanted messages impede other services or result in extra charges.
- Electronic tracking: pinpointing of a user's location via his device.
- Exposure: direct release of sensitive data to an unauthorized entity. Examples: data scavenging, human error, system error, sale of personal information.
- Interception: an unauthorized entity directly accesses data transiting between authorized sources and destinations. Examples: theft, wiretapping, emanations analysis.
- Inference: an unauthorized entity indirectly accesses sensitive data (possibly information besides the data itself) by reasoning from characteristics or byproducts of communications. For example, exploiting covert channels via communications traffic analysis or signals analysis.

¹²⁵ Sources: (NIST, 2002), (IETF, 2000), and (NIST, 2008).

- Intrusion: an unauthorized entity bypasses or subverts authentication mechanisms to access sensitive data. Examples: trespassing, system penetration, reverse engineering, cryptanalysis, social engineering
- Masquerade: an unauthorized entity poses as an authorized entity to gain access to a system or performs a malicious act. Examples: masquerading via spoofing or malicious logic, system cloning.
- Falsification: false data deceives an authorized party. Examples: data substitution, insertion, fabrication, and modification.
- Repudiation: false denial of an action. Examples: falsely denying the origin or receipt of a message.
- Incapacitation: disabling a system component to prevent or interrupt system operation. Examples: equipment loss or theft, malicious logic, physical destruction (sabotage), human error, hardware/software error, denial of service.
- Corruption: undesirable alteration of system operation through an adverse modification of system functions or data. Examples: tampering, malicious logic, human error, system error.
- Obstruction: hindering system operations to interrupt delivery of system services. Examples: interference (blocking communications), causing an overload of resources, signal jamming.
- Misappropriation: unauthorized assumption of logical or physical control of a system resource. Examples: theft of service, functionality, or data.
- Misuse: causing a system component to perform in away that is detrimental to system security. Examples: tampering, malicious logic, and escalation of privileges.

2. Vulnerabilities

Organizations may implement security controls through technology, management or operations (NIST, 1995). Given that vulnerabilities include technical, management, and operational flaws (Internet Engineering Task Force [IETF], 2000), the set of vulnerabilities for a system can be described as consisting of a lack of security controls. A vulnerability may also exist if the implementation of a security control lacks

robustness—that is, enforced to an insufficient degree. The following list provides a compilation of general security controls for both systems and networks:¹²⁶

- Identification and authentication: Verification of a subject's¹²⁷ identity ensures that identity's validity. Examples include passwords, personal identification numbers, and methods of strong authentication (e.g., token, smart card, digital certificate, and Kerberos).
- Authorization: Authorization enables specification and management of a subject's allowed actions.
- Access controls enforcement: In short, ensuring authorized subjects conform to system security policy via access control mechanisms (e.g., sensitivity labels; file permissions, access control lists, roles, and user profiles). Access control effectiveness depends on system security design and the configuration of security rules.
- Nonrepudiation: Spanning both prevention and detection, this control is typically applied at the point of message transmission or reception.
- Protected Communications: Using encryption and cryptographic technologies to facilitate trustworthy communications, ensure the integrity, availability, and confidentiality of information in transit, and mitigate network threats.
- Transaction Privacy: Using controls such as Secure Sockets Layer to protect against loss of privacy.
- Management controls: Examples include security policy, risk management, security planning, and assurance (design, implementation, and operational).
- Operational controls: Examples include organizational training and education, contingency and disaster preparation, incident handling, and physical and environmental security.
- Audit trail maintenance.
- Protection of server resident data: Content, such as electronic mail, maintained by a third party may expose sensitive information through the third-party server's vulnerabilities.

¹²⁶ Note: Systems may implement security controls to varying degrees. This list is based on discussions and examples in NIST (1995, 2000, and 2008).

¹²⁷ A subject is a system entity that either causes information flow between system objects or effects changes in the system state (IETF, 2008).

3. Impacts

Quantitative estimates may represent tangible impacts in the form of lost revenue or equipment repair costs; however, other impacts, such as damage to organizational interests, may best be measured qualitatively (NIST, 2002). The following list describes potential system impacts in terms of a loss or degradation of confidentiality, integrity, and availability (NIST, 2002):

- Confidentiality: The impact of an unauthorized information disclosure can range from a loss of personal privacy to the jeopardizing of national security. It could also precipitate public embarrassment or legal action against the organization.
- Integrity: A compromise of integrity could lead to erroneous decisions or cascading degradation to system availability or confidentiality.
- Availability: Losses here may result in reduced productivity, ultimately reducing organizational effectiveness.

B. MEASURING SYSTEM VULNERABILITY

The Common Criteria represents a widely acknowledged methodology for evaluating the assurance level of an information system. Assuming that evaluations for higher assurance levels assess potential system vulnerabilities more rigorously than those for lower assurance levels, meeting higher assurance requirements indicates reduced vulnerability for a given system. Furthermore, the Common Criteria addresses protection of assets in terms of confidentiality, integrity, and availability.¹²⁸ The authors of this work leverage the Common Criteria EALs, summarized in Table 20, to estimate vulnerability levels of various systems and relate them to one another.

¹²⁸ Common Criteria Recognition Arrangement. (2009). *Common criteria for information technology security evaluation part 1: Introduction and general model*. Retrieved from <http://www.commoncriteriaportal.org/ccra>.

EAL	Summary Description
1: functionally tested	Evidence that the system functions in a manner consistent with its documentation.
2: structurally tested	A low to moderate level of independently assured security.
3: methodically tested and checked	A moderate level of independently assured security.
4: methodically designed, tested, and reviewed	A moderate to high level of independently assured security in conventional commodity TOEs
5: semiformally designed and tested	A high level of independently assured security in a planned development
6: semiformally verified design and tested	High assurance from application of security engineering techniques to a rigorous development environment
7: formally verified design and tested	High assurance from extensive formal analysis

Table 20. Common Criteria Evaluation Assurance Levels¹²⁹

¹²⁹ Source: Common Criteria Recognition Arrangement. (2009). *Common criteria for information technology security evaluation part 3: Security assurance requirements*. Retrieved from <http://www.commoncriteriaportal.org/ccra>.

APPENDIX B. DOD WIRELESS CONTRACTS

A. ELECTRONIC DATA SYSTEM CONTRACT TRENDS

Figure 50 illustrates the breakdown of expenses over the previous 4 years against the EDS contract. NMCI charges a monthly fixed cost to remotely access their network—the majority of the NMCI expenses are associated with this cost. The NMCI contract charges this overhead to offset the operating cost of these services. The other contracts do not include these end-subscriber charges, potentially because the operating cost is realized as manpower sunk cost (i.e., the local installations provide the services vice a contractor). Another interesting trend is the difference in market distribution; unlike the commercial market (i.e., where Verizon receives the most revenue), AT&T receives twice the EDS procurements as Verizon. The reason for this anomaly is unknown—especially since the other Navy/Marine Corps contract (i.e., NDWC) is completely different.

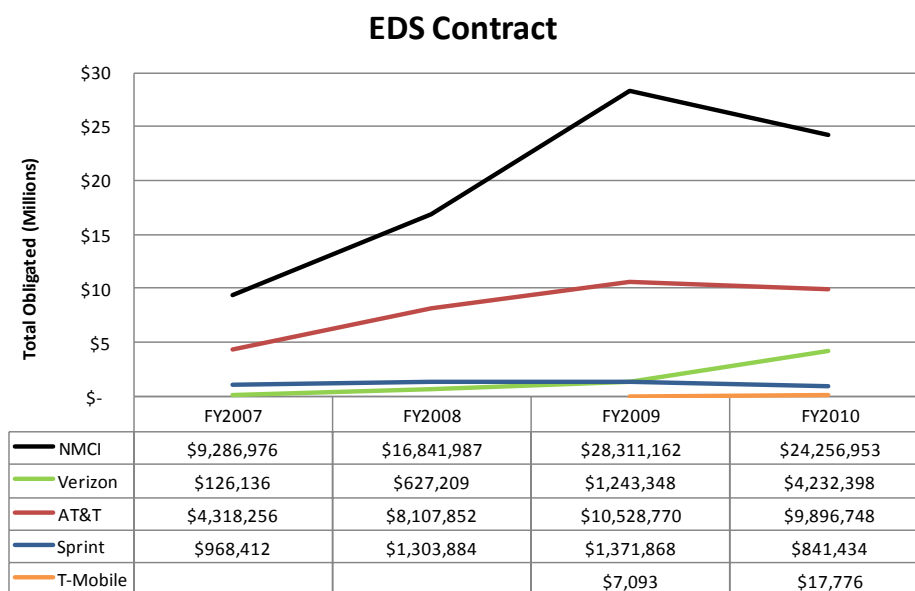


Figure 50. EDS Contract¹³⁰

¹³⁰ Contract totals obtained from extracting and aggregating the data from https://www.fpds.gov/fpdsng_cms/ (Federal Procurement Data System – Next Generation).

B. NATIONAL DEPARTMENT OF THE NAVY WIRELESS CONTRACTS TRENDS

Figure 51 represents the procurement trends under the NDWC contracts for cellular services and equipment between the years of FY05 and FY10. Overall, the graph illustrates a steady increase in procurements for cellular services and equipment. One note for this chart is the change in procurement behaviors between FY08 and FY09 under the AT&T contract, and under the Sprint contract between FY06 and FY09. These changes in behavior might be indicative of Verizon acquiring Alltel in 2008 and Sprint losing its market share since 2006 (Pyramid Research, 2009). The procurements against these contracts are more representative of the commercial market trends.¹³¹

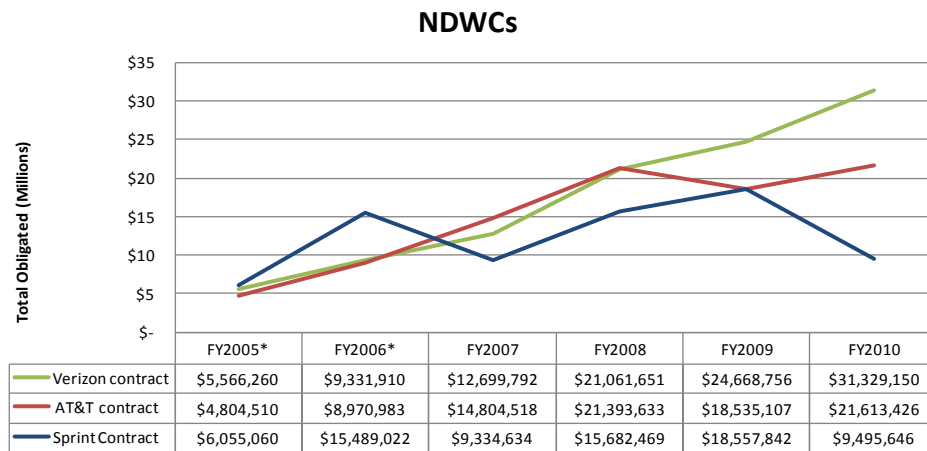


Figure 51. NDWC Contracts¹³²

C. ARMY AIR FORCE BLANKET PURCHASE AGREEMENTS TRENDS

Figure 52 represents the cellular services and equipment procurements through the AAFBPAs. The procurement totals were not available for any year prior to FY07. The graph illustrates a significant difference between service providers—AT&T and Verizon are represented as dominating the market. Note the differences in trends across the EDS, NDWCs, and the AAFBPAs. This data suggests that the EDS contract favored

¹³¹ Appendix H – illustrates the distributions of commercial vendors operating wireless revenues.

¹³² Contract totals obtained from extracting and aggregating the data from <https://www.fpds.gov/fpdsng.cms/> (Federal Procurement Data System – Next Generation)

AT&T, which is different from the commercial market share. USA Mobility and Worldcell were contracted only for the procurement of data cards. Therefore, the delivery order totals are expected to be less than those of the other vendors.

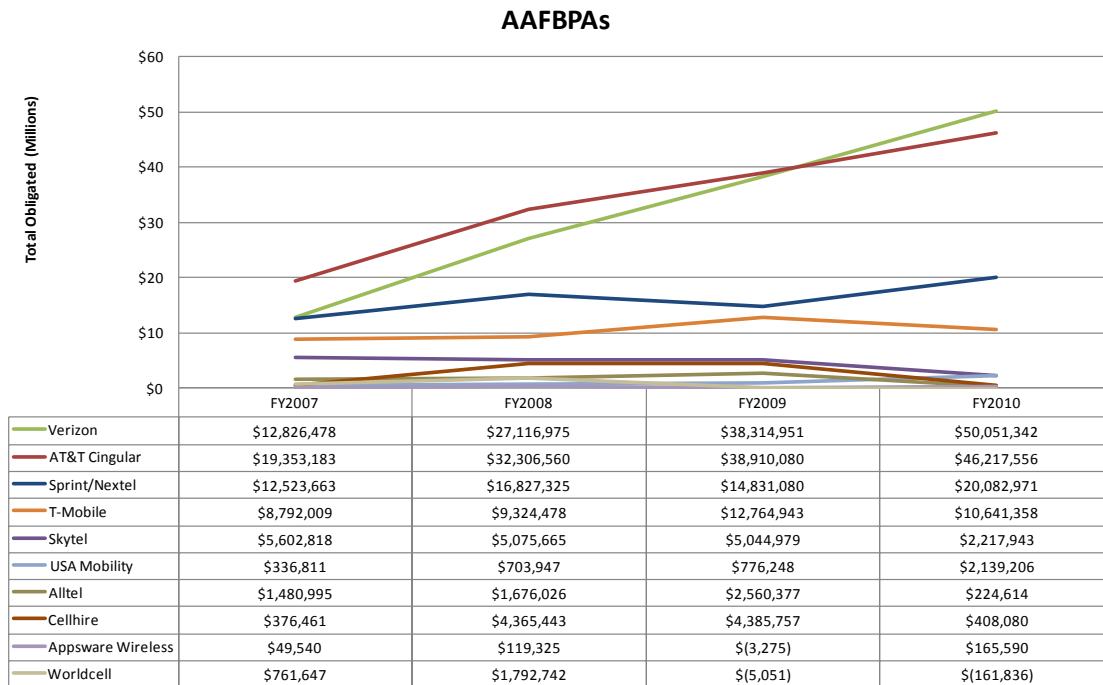


Figure 52. AAFBPA Contracts¹³³

In summary, these contracts are grossly disjointed. As a research firm suggests in its report on managing wireless costs, the best-in-class corporations (i.e., top-rated corporations for managing wireless expenses), have complete control of their entire inventory of wireless devices, automate the policy enforcement, and maintain a holistic view of all usage rates. After consulting with a large wireless services negotiation firm, their number one recommendation for reducing cost was to consolidate the contracting (Brill Worldwide Investments, 2010). Centrally managing the sourcing strategy provides a number of advantages. As this is not the main focus of the paper, the discussion will not digress any further; however, investigation of the use of wireless negotiation firms is recommended for future sourcing initiatives.

¹³³ Contract totals obtained from extracting and aggregating the data from https://www.fpbs.gov/fpbsng_cms/ (Federal Procurement Data System – Next Generation)

Tables 21 through 24 present detailed supporting information pertaining to the figures presented above.

	FISC NDWC			
	AT&T contract	Sprint Contract	Verizon contract	FISC Total
FY2005*	\$ 5,468,206	\$ 7,736,418	\$ 6,268,492	\$ 19,473,117
FY2006*	\$ 9,338,364	\$ 15,778,150	\$ 12,936,616	\$ 38,053,130
FY2007	\$ 12,536,322	\$ 14,877,205	\$ 19,410,131	\$ 46,823,658
FY2008	\$ 19,878,715	\$ 15,394,125	\$ 21,724,494	\$ 56,997,334
FY2009	\$ 18,536,925	\$ 15,687,356	\$ 25,293,494	\$ 59,517,776
FY2010	\$ 21,613,426	\$ 9,495,646	\$ 31,329,150	\$ 62,438,221
Total	\$ 87,371,958	\$ 78,968,901	\$ 116,962,376	\$ 283,303,236

Table 21. FISC NDWC Contract Summary by Network Operator

	NMCI EDS					
	NMCI	AT&T	Sprint	Verizon	T-Mobile	EDS Total
FY2005*						\$ 5,000,000
FY2006*						\$ 10,000,000
FY2007	\$ 9,286,976	\$ 4,318,256	\$ 968,412	\$ 126,136		\$ 14,699,780
FY2008	\$ 16,841,987	\$ 8,107,852	\$ 1,303,884	\$ 627,209		\$ 26,880,933
FY2009	\$ 28,311,162	\$ 10,528,770	\$ 1,371,868	\$ 1,243,348	\$ 7,093	\$ 41,462,241
FY2010	\$ 24,256,953	\$ 9,896,748	\$ 841,434	\$ 4,232,398	\$ 17,776	\$ 39,245,310
Total	\$ 78,697,078	\$ 32,851,627	\$ 4,485,599	\$ 6,229,092	\$ 24,869	\$ 137,288,264

Table 22. NMCI EDS Contract Summary by Network Operator

	ITEC4 AAFBPA										
	Alltel	AT&T Cingular	Cellhire	Skytel	Sprint/Nextel	T-Mobile	USA Mobility	Verizon	Worldcell	Appsware Wireless	Army AF Total
FY2005*											\$ 25,000,000
FY2006*											\$ 40,000,000
FY2007	\$ 1,480,995	\$ 21,085,608	\$ 376,461	\$ 5,602,818	\$ 12,690,740	\$ 8,821,095	\$ 336,811	\$ 13,097,209	\$ 761,647	\$ 49,540	\$ 64,302,923
FY2008	\$ 1,676,026	\$ 31,440,807	\$ 4,365,443	\$ 5,075,665	\$ 16,362,387	\$ 9,190,055	\$ 703,947	\$ 26,800,641	\$ 1,792,742	\$ 119,325	\$ 97,527,037
FY2009	\$ 2,560,377	\$ 39,656,976	\$ 4,385,757	\$ 5,044,979	\$ 15,282,822	\$ 12,891,759	\$ 776,248	\$ 38,972,801	\$ (5,051)	\$ (3,275)	\$ 119,563,392
FY2010	\$ 224,614	\$ 46,217,556	\$ 408,080	\$ 2,217,943	\$ 20,082,971	\$ 10,641,358	\$ 2,139,206	\$ 50,051,342	\$ (161,836)	\$ 165,590	\$ 131,986,823
Total	\$ 5,942,011	\$ 138,400,947	\$ 9,535,741	\$ 17,941,405	\$ 64,418,919	\$ 41,544,267	\$ 3,956,212	\$ 128,921,992	\$ 2,387,502	\$ 331,180	\$ 478,380,175

Table 23. AAFBPA Contract Summary by Network Operator

	Commerical Operating Revenue (Wireless)				
	AT&T Revenue	Sprint Revenue	Verizon Revenue	T-Mobile Revenue	Total
2004	\$ 19,565,000,000	\$ 13,137,000,000	\$ 27,662,000,000	\$ 11,680,000,000	\$ 72,044,000,000
2005	\$ 34,468,000,000	\$ 20,181,000,000	\$ 32,301,000,000	\$ 14,806,000,000	\$ 101,756,000,000
2006	\$ 37,537,000,000	\$ 31,918,000,000	\$ 38,043,000,000	\$ 17,138,000,000	\$ 124,636,000,000
2007	\$ 42,684,000,000	\$ 32,105,000,000	\$ 43,882,000,000	\$ 19,288,000,000	\$ 137,959,000,000
2008	\$ 49,335,000,000	\$ 28,435,000,000	\$ 49,332,000,000	\$ 21,885,000,000	\$ 148,987,000,000
2009	\$ 53,597,000,000	\$ 25,832,000,000	\$ 62,131,000,000	\$ 21,531,000,000	\$ 163,091,000,000

Table 24. Revenue of Top Four MNOs

APPENDIX C. MVNO COSTS

The following tables provide a full list of services and costs associated with MVNOs. Those services were used as a basis for developing cost estimates.

Revenue	COGS
<i>Population & penetration</i>	<i>SIM cards</i>
population growth in period	new SIM cards issued
total population	SIM cards replacement % in period
Mobile penetration growth in period	Total SIM cards issued in period
total mobile penetration (%)	<i>SIM card cost</i>
Mobile users	SIM Card cost per unit
<i>Prices & margins</i>	SIM card shrinkwrap cost per unit
Minute	SIM card shipping cost per unit
Messaging	<i>Cost to operators</i>
Data	Cost to operator per minute
<i>Content contribution</i>	Cost to operator per message
value of content download per user per month	Cost to operator per mbyte
<i>International calls contribution</i>	<i>cost of minutes bundling</i>
% user who make international calls	minutes
avg. monthly minutes of int. traffic per user	messages
average minute cost for int. calls	data
<i>Monthly fees per user</i>	<i>Various notification costs</i>
Monthly minute fees per user	notifications per user per period
Monthly SMS fees per user	notification cost per period
Monthly MMS fees per user	<i>Subscriber usages</i>
Monthly GPRS fees per user	total Customers minute usage in period
Monthly content revenues per user	accumulated quaterly/yearly minutes
Monthly int. calling revenues per user	accumulated minutes usage
<i>ARPU levels</i>	
monthly ARPU (excluding starter packages)	
quarterly ARPU (excluding starter packages)	
yearly ARPU (excluding starter packages)	
<i>HR Cost</i>	
Cust. Serv. Reps.	
Back-office outsourcing - per mpl.	
Mobile phone usage cost - per empl.	
fixed phone cost - per empl	
*Supply Management included	

Table 25. Typical MVNO Costs

CAPEX	Other Cost
Hardware boxes	Communication costs
boxes for data comm.	leased lines (office connection)
equipment for SS7 comm.	leased lines (operations connection)
IT for web front-end	fixed phone costs
IT for service management	mobile costs
IT for usage control & notification	IT service cost
IT for billing/financial management	external consultants (web front end)
IT for SIM card pre-activation	Voice-mail consulting fees
IT for CDR post-processing	IT service (running support for office IT)
IT for fraud system	IT installation services - operations IT
Misc other hardware	SW License fees + one-time fees
Software platforms	Billing & CC software (see notes)
SW for CC Modules	interconnect fee - payment provider
Call center PBX cost	vendor downpayments + integration
SW for usage control & notification	CC hotline + SLA fees
SW for billing/financial management	bank guarantees
SW for SIM card pre-activation	Hosted services cost
SW for CDR post-processing	Hosting - CC & Billing servers
HLR SW	Hosting - office system
ERP finance system	Hosting - database server
IT platform	
ERP software	
Furniture & office investments	
Direct empl. related office costs (furniture)	
Other furniture and misc. to office	
Office platforms - HW	
Laptops & stationary PC (incl. Monitor)	
Office mail server	
Other office IT related (firewall, backup)	
Misc other hardware	
Mobiles	
Printers (smaller)	
Other equipment to office	

Table 26. Typical MVNO Capital Expenditure and Other Costs

APPENDIX D. MILITARY END STRENGTH AND PAY CHART

militarypay.defense.gov						End Strength				Total		
	Annual Basic	BAS	BAH	Total	hourly rate	USN	USAF	USA	USMC	End Strength	Annual Cost	Hourly Cost
E-1 (less than 2)	\$17,604	\$3,900	\$9,600	\$31,104	\$16.20	15385	10541	22342	11277	59545	\$1,852,116,261.60	\$964,643.89
E-2 (less than 2)	\$19,740	\$3,900	\$10,800	\$34,440	\$17.94	18688	7003	33939	25479	85109	\$2,931,194,812.32	\$1,526,663.96
E-3 (over 2)	\$22,068	\$3,900	\$12,000	\$37,968	\$19.78	38185	48152	60319	44963	191619	\$7,275,482,169.12	\$3,789,313.63
E-4 (over 3)	\$25,476	\$3,900	\$13,200	\$42,576	\$22.18	50819	50211	141958	37749	280737	\$11,952,793,265.76	\$6,225,413.16
E-5 (over 4)	\$29,376	\$3,900	\$14,400	\$47,676	\$24.83	67520	71123	84132	29646	252421	\$12,034,544,758.08	\$6,267,992.06
O-1 (less than 2)	\$33,396	\$2,686	\$14,400	\$50,482	\$26.29	6836	6648	10788	3505	27777	\$1,402,240,736.16	\$730,333.72
W-1 (over 6)	\$41,340	\$2,686	\$14,400	\$58,426	\$30.43	1688		3126	258	5072	\$296,337,077.76	\$154,342.23
E-6 (over 7)	\$40,584	\$3,900	\$15,600	\$60,084	\$31.29	46588	42146	65605	16853	171192	\$10,285,982,300.16	\$5,357,282.45
O-2 (over 2)	\$43,836	\$2,686	\$16,800	\$63,322	\$32.98	7020	7203	7970	3401	25594	\$1,620,665,315.52	\$844,096.52
E-7 (over 12)	\$45,012	\$3,900	\$16,800	\$65,712	\$34.23	21586	26341	42237	9133	99297	\$6,525,052,126.56	\$3,398,464.65
W-2 (over 8)	\$48,708	\$2,686	\$16,800	\$68,194	\$35.52	535		5533	808	6876	\$468,902,494.08	\$244,220.05
E-8 (over 14)	\$50,292	\$3,900	\$18,000	\$72,192	\$37.60	6525	5286	1270	4015	17096	\$1,234,202,638.08	\$642,813.87
W-3 (over 12)	\$57,432	\$2,686	\$19,200	\$79,318	\$41.31	556		3592	454	4602	\$365,021,804.16	\$190,115.52
O-3 (over 4)	\$59,424	\$2,686	\$19,200	\$81,310	\$42.35	15670	22431	26401	5744	70246	\$5,711,707,879.68	\$2,974,847.85
E-9 (over 16)	\$60,348	\$3,900	\$19,200	\$83,448	\$43.46	2712	2635	3593	1595	10535	\$879,129,736.80	\$457,880.07
W-4 (over 16)	\$66,360	\$2,686	\$21,600	\$90,646	\$47.21	564		2676	275	3515	\$318,620,971.20	\$165,948.42
O-4 (over 8)	\$70,956	\$2,686	\$21,600	\$95,242	\$49.61	10311	14773	18097	3910	47091	\$4,485,044,789.28	\$2,335,960.83
W-5 (over 20)	\$81,852	\$2,686	\$24,000	\$108,538	\$56.53	33		570	107	710	\$77,062,036.80	\$40,136.48
O-5 (over 12)	\$82,668	\$2,686	\$24,000	\$109,354	\$56.96	6805	9899	9853	1894	28451	\$3,111,232,930.08	\$1,620,433.82
O-6 (over 14)	\$91,716	\$2,686	\$26,400	\$120,802	\$62.92	3414	3509	4670	673	12266	\$1,481,758,313.28	\$771,749.12
O-7 (over 16)	\$129,576	\$2,686	\$28,800	\$161,062	\$83.89	107	146	153	35	441	\$71,028,377.28	\$36,993.95
O-8 (over 18)	\$147,492	\$2,686	\$31,200	\$181,378	\$94.47	69	101	90	24	284	\$51,511,374.72	\$26,828.84
O-9 (over 20)	\$161,640	\$2,686	\$33,600	\$197,926	\$103.09	33	38	53	15	139	\$27,511,725.12	\$14,329.02
O-10 (over 22)	\$185,712	\$2,686	\$36,000	\$224,398	\$116.87	9	14	12	4	39	\$8,751,525.12	\$4,558.09
				\$2,165,604		321658	328200	548979	201817	1400654	\$74,467,895,418.72	\$38,785,362.20

Table 27. Military End Strength and Pay for Each Service (From <http://militarypay.defense.gov>)

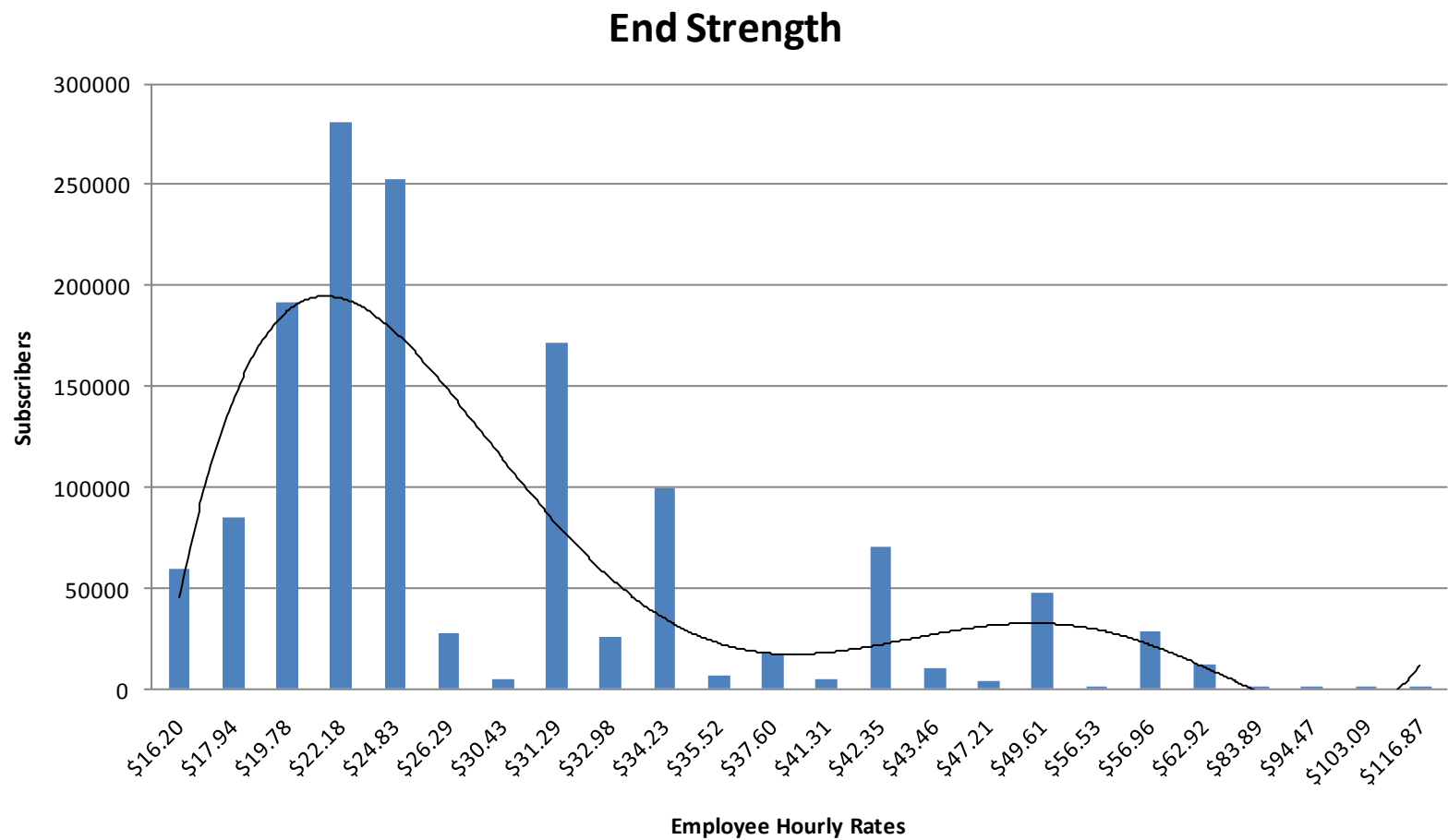




Table 28. Distribution of Military End Strength by Hourly Pay Rate

APPENDIX E. SECURE MOBILE ENVIRONMENT PORTABLE ELECTRONIC DEVICE FEATURES

The following table provides a brief list of the SME PED features: ¹³⁴

		
	General Dynamics – Sectera Edge	L-3 – Guardian
Operating System	Windows CE	Windows CE
Display	TFT QVGA 2.8in., 64k colors	High Res. LCD 3in.,
Memory	Unclass. Flash 128MB, RAM 64MB; Class. Flash 64MB, RAM 64MB; MicroSD up to 2GB	Dynamic Allocated across Unclass. And Class. 256MB; MicroSD (up to 8 cards)
Wireless Interface	GSM EDGE, UMTS, HSDPA, CDMA 1xRTT, EVDO Rev. A, 802.11 b/g	GSM EDGE, UMTS, HSDPA, CDMA 1xRTT, EVDO Rev. 0&A, 802.11 b/g, 802.15.1
Battery Life	Lithium-Ion Standby ~60 hrs, Talk ~5 hrs, Secure Talk ~3hrs	Lithium Polymer Standby ~50 hrs, Talk ~4 hrs, Extended battery provides more
CAC Enabled	DoD PKI	DoD PKI
Security Protocols	SCIP, HAIPE, Suite A/B Type 1 and non-Type 1	SCIP, HAIPE IS, Suite A/B Type 1 and non-Type 1
Weight	12 oz	13 oz
Environmental	MIL-STD-810F	MIL-STD-810F
Purchase Price	~\$4000 includes accessories and mail client	~\$4000 includes accessories and mail client
R&D Expenses	Government proportion: \$38M + \$5M Upgrades (GD only)¹³⁵	

¹³⁴ General Dynamics C4 Systems, 2010; L-3 Communications Systems-East, 2008.

¹³⁵ NSA program office provided totals.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F. DOD PROCUREMENTS BY AREA

Figure 53 illustrates the distribution of DoD procurements for FY2010 by funding office location. According to the procurement trends, Virginia accounted for the top 25%, Georgia and D.C. accounted for the next 25%, the yellow states accounted for the next 25%, and the blue states accounted for another 23%. Even though some of the green colored states contain highly concentrated military installations, they provide only 3% of the demand. This suggests that wireless demand is not closely correlated to military base end strengths. Additionally, this suggests that DoD procurements are not evenly distributed across the country—specific areas are more likely than others to purchase high quantities of services. Essentially, this data suggests that the majority of the DoD’s demand is distributed around specific DoD procurements are closely aligned by regions.

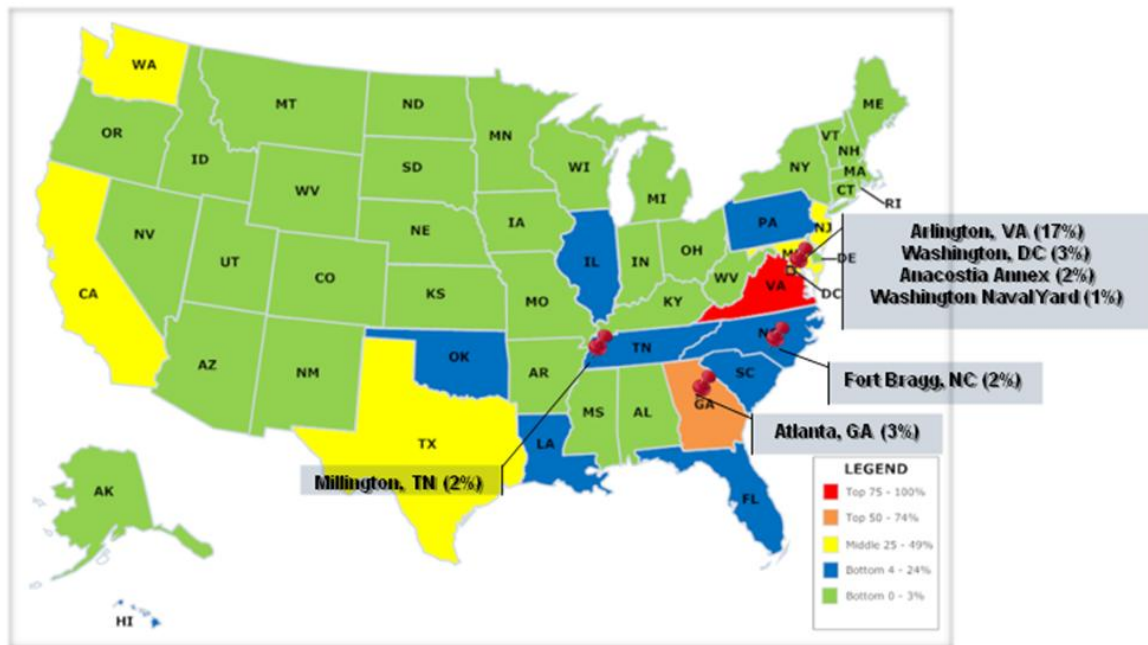


Figure 53. NDWC and AAFPBA Procurement Distribution

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX G. CELLULAR NETWORK ARCHITECTURE

Figure 54 illustrates the common, integrated mobile network architecture. If the DoD implements the MVNO approaches, the blue arrow illustrates the proportions of the cellular architectures the organization would need to adopt. Each cellular architecture is listed by generation.

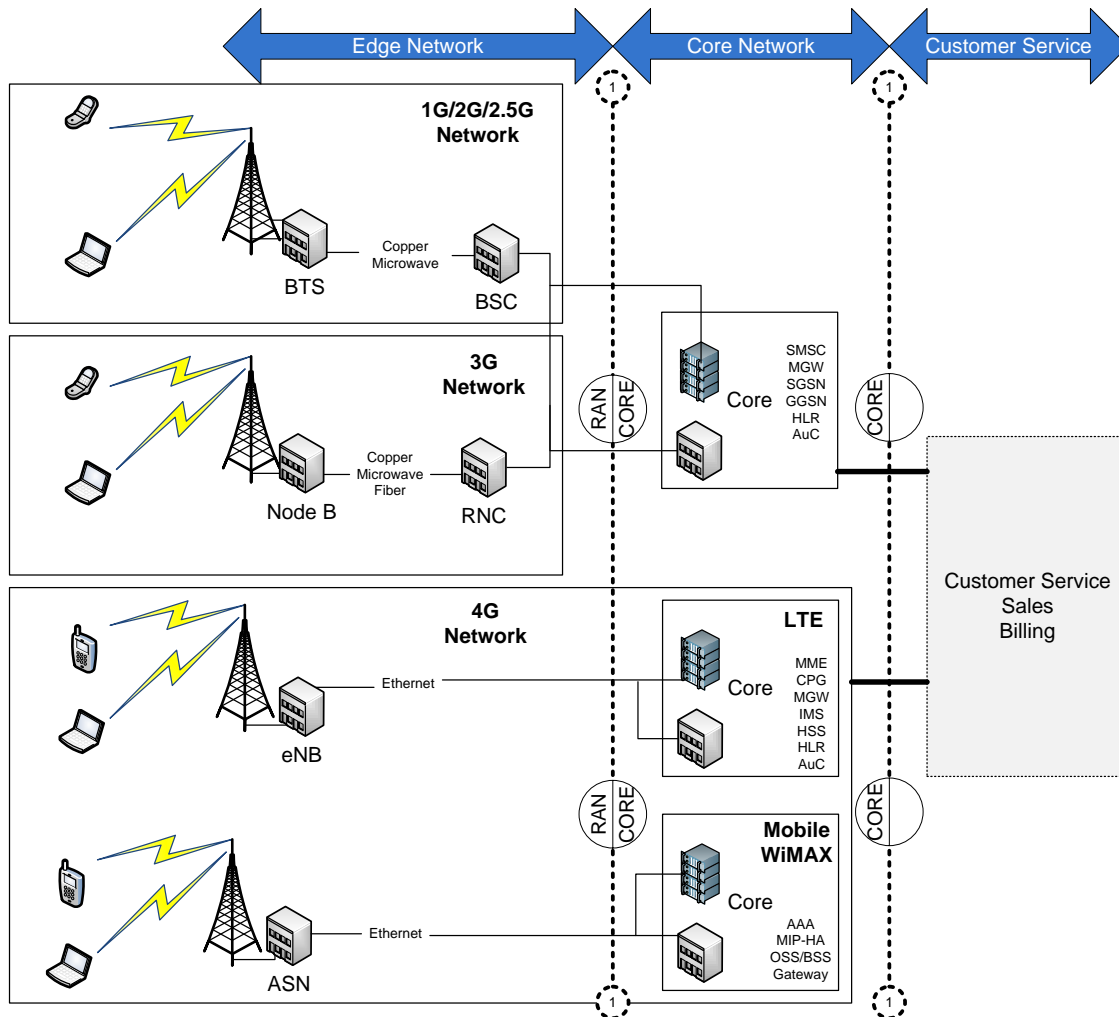


Figure 54. 2G/3G/4G Cellular Architecture¹³⁶

¹³⁶ Network Strategy Partners (2009); Pressley (2010).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX H. PRODUCTIVITY RECOVERY CHARTS

The following tables enumerate the costs for various ranges of productivity increases given varying numbers of users (subscribers):

1 to 400K subscribers (FY2010)				
Gamma Distribution				
Productivity Increases	Expected (per day)	Expected (annually)	Minimum (per day)	Minimum (annually)
1 - 10 Mins	\$ 94,776	\$ 22,746,240	\$ 38,030	\$ 9,127,200
11 - 20 Mins	\$ 423,422	\$ 101,621,280	\$ 162,115	\$ 38,907,600
21 - 30 Mins	\$ 731,530	\$ 175,567,200	\$ 274,357	\$ 65,845,680
31 - 60 Mins	\$ 1,238,500	\$ 297,240,000	\$ 470,253	\$ 112,860,720
1 to 500K subscribers (FY2012)				
Productivity Increases	Expected (per day)	Expected (annually)	Minimum (per day)	Minimum (annually)
1 - 10 Mins	\$ 114,526	\$ 27,486,240	\$ 45,874	\$ 11,009,760
11 - 20 Mins	\$ 520,213	\$ 124,851,120	\$ 198,844	\$ 47,722,560
21 - 30 Mins	\$ 891,388	\$ 213,933,120	\$ 327,955	\$ 78,709,200
31 - 60 Mins	\$ 1,523,750	\$ 365,700,000	\$ 573,769	\$ 137,704,560
1 to 600K subscribers (FY2014)				
Productivity Increases	Expected (per day)	Expected (annually)	Minimum (per day)	Minimum (annually)
1 - 10 Mins	\$ 134,406	\$ 32,257,440	\$ 54,200	\$ 13,008,000
11 - 20 Mins	\$ 608,165	\$ 145,959,600	\$ 231,456	\$ 55,549,440
21 - 30 Mins	\$ 1,041,566	\$ 249,975,840	\$ 388,082	\$ 93,139,680
31 - 60 Mins	\$ 1,748,913	\$ 419,739,120	\$ 661,057	\$ 158,653,680
1 to 700K subscribers (FY2016)				
Productivity Increases	Expected (per day)	Annual Expected	Minimum (per day)	Annual Minimum
1 - 10 Mins	\$ 161,933	\$ 38,863,920	\$ 65,283	\$ 15,667,920
11 - 20 Mins	\$ 733,202	\$ 175,968,480	\$ 275,603	\$ 66,144,720
21 - 30 Mins	\$ 1,234,957	\$ 296,389,680	\$ 472,179	\$ 113,322,960
31 - 60 Mins	\$ 2,072,203	\$ 497,328,720	\$ 790,525	\$ 189,726,000

Table 29. Productivity Savings Estimates for Between 1 and 700K Subscribers

300K to 400K subscribers (FY2010)				Expected 340K
Productivity Increases	Expected (per day)	Expected (annually)	Minimum (per day)	Minimum (annually)
1 - 10 Mins	\$ 678,882	\$ 162,931,680	\$ 276,768	\$ 66,424,320
11 - 20 Mins	\$ 2,633,840	\$ 632,121,600	\$ 1,458,187	\$ 349,964,880
21 - 30 Mins	\$ 4,180,651	\$ 1,003,356,240	\$ 2,563,484	\$ 615,236,160
31 - 60 Mins	\$ 7,785,020	\$ 1,868,404,800	\$ 4,717,347	\$ 1,132,163,280
400K to 500K subscribers (FY2012)				Expected 460K
Productivity Increases	Expected (per day)	Expected (annually)	Minimum (per day)	Minimum (annually)
1 - 10 Mins	\$ 814,259	\$ 195,422,160	\$ 365,820	\$ 87,796,800
11 - 20 Mins	\$ 3,468,154	\$ 832,356,960	\$ 2,137,182	\$ 512,923,680
21 - 30 Mins	\$ 5,481,537	\$ 1,315,568,880	\$ 3,474,686	\$ 833,924,640
31 - 60 Mins	\$10,187,230	\$ 2,444,935,200	\$ 6,180,598	\$ 1,483,343,520
500K to 600K subscribers (FY2014)				Expected 580K
Productivity Increases	Expected (per day)	Expected (annually)	Minimum (per day)	Minimum (annually)
1 - 10 Mins	\$ 996,652	\$ 239,196,480	\$ 451,679	\$ 108,402,960
11 - 20 Mins	\$ 4,281,470	\$ 1,027,552,800	\$ 2,643,735	\$ 634,496,400
21 - 30 Mins	\$ 6,796,365	\$ 1,631,127,600	\$ 4,568,085	\$ 1,096,340,400
31 - 60 Mins	\$12,398,817	\$ 2,975,716,080	\$ 7,448,090	\$ 1,787,541,600
600K to 700K subscribers (FY2016)				Expected 697K
Productivity Increases	Expected (per day)	Expected (annually)	Minimum (per day)	Minimum (annually)
1 - 10 Mins	\$ 1,318,356	\$ 316,405,440	\$ 543,915	\$ 130,539,600
11 - 20 Mins	\$ 5,098,538	\$ 1,223,649,120	\$ 3,153,427	\$ 756,822,480
21 - 30 Mins	\$ 7,989,305	\$ 1,917,433,200	\$ 5,432,212	\$ 1,303,730,880
31 - 60 Mins	\$14,891,836	\$ 3,574,040,640	\$ 9,117,837	\$ 2,188,280,880

Table 30. Productivity Savings Estimates for Between 300K and 700K Subscribers

The lines in the following figures represent the savings from the minutes that may be potentially recovered from an increase in productivity.

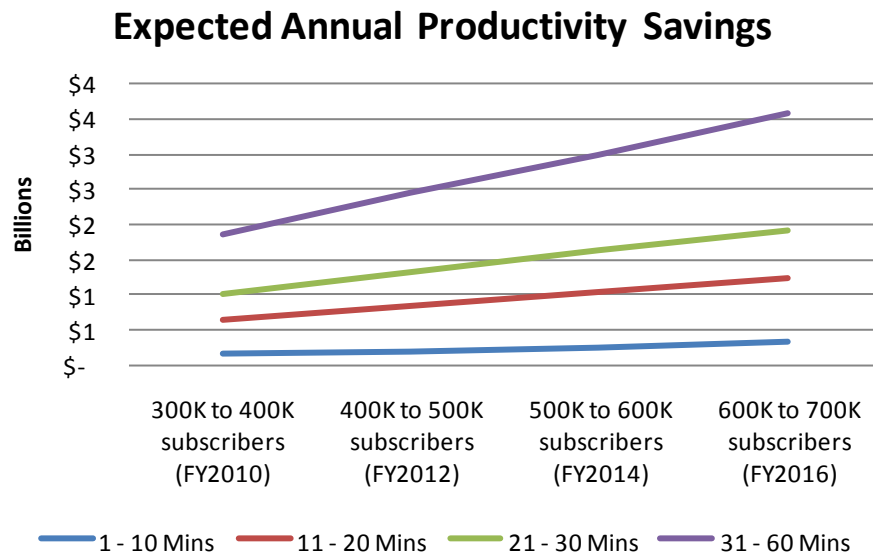


Figure 55. Expected Productivity Savings for 300K to 700K Subscribers

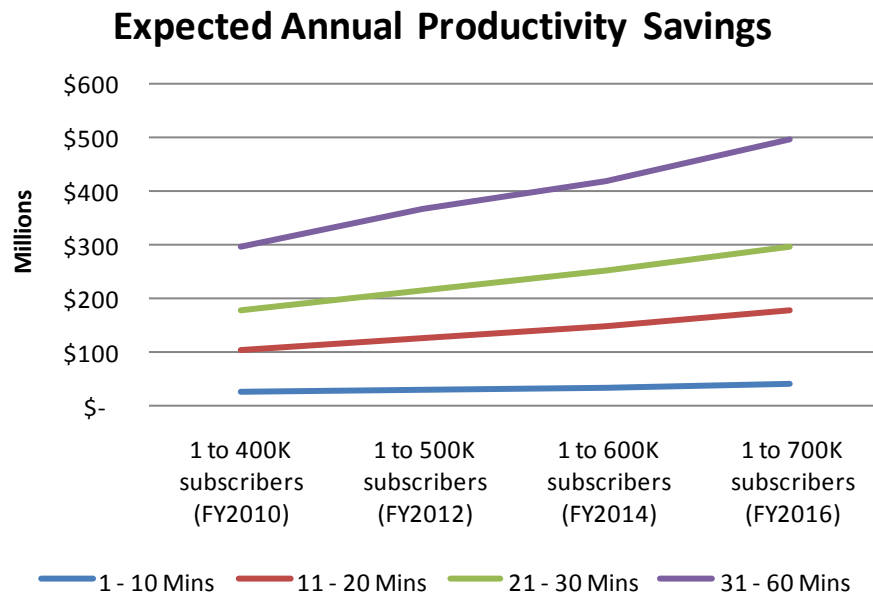


Figure 56. Expected Productivity Savings for 1 to 700K Subscribers

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX I. IN-DEPTH RISK ASSESSMENT

This section provides an example of a more in-depth risk assessment than that performed in Chapter IV to estimate the risk levels of potential network service business cases. A precondition for an in-depth risk assessment of each case is identification of a likely architecture. The architecture drives the system vulnerabilities, and it may contain elements that naturally reduce the likelihood of successful, or attempted, threat actions. A detailed risk assessment will provide a much more granular depiction of the threats and vulnerabilities inherent within candidate architectures, and it will contribute to the ultimately choosing the most beneficial business case.

A. THREAT

Threat actions are defined and listed in Appendix A. They are essentially a method that exploits or triggers vulnerabilities. Based on the network concepts presented in Chapter IV, Table 21 depicts the potential of a threat action. The numbers 0, 1, and 2 represent high, medium, and low threat, respectively. In accordance with (NIST, 2002) the following sections describe the level of threats per each category listed in Table 21.

Threat Actions	Commercial MNO (Retail)	Commercial MNO w/ MCEP	RAN (only edge network)	Enhanced WiFi (Garrison)	Customer Service, Sales, Billing	Integrated VM and Messaging	Edge Network w/ Commercial Core	Core Network w/ Edge Network	DoD MNO	Mobile Base Station	Enhanced WiFi (Tactical)	Tethered Tactical Networks	Tactical Waveform Sleeve
Natural Threats	0	0	0	0	0	0	0	0	0	1	1	1	1
Environmental Threats	0	0	0	0	0	0	0	0	0	0	0	0	0
Service Abuse	0	0	0	1	0	0	0	0	0	1	1	1	1
Backdoor	0	0	0	0	0	0	0	0	0	0	0	0	0
Electronic Tracking	0	0	0	0	0	0	1	1	1	1	1	1	1
Exposure	0	0	0	0	0	0	0	0	0	0	0	0	0
Interception	0	0	0	0	0	0	0	0	0	1	1	1	1
Inference	0	0	0	0	0	0	0	0	0	0	0	0	0
Intrusion	0	0	0	0	0	0	0	0	0	0	0	0	0
Masquerade	0	0	0	0	0	0	0	0	0	0	0	0	0
Falsification	0	0	0	0	0	0	0	0	0	0	0	0	0
Repudiation	0	0	0	0	0	0	0	0	0	0	0	0	0
Incapacitation	0	0	0	0	0	0	0	0	0	0	0	0	0
Corruption	0	0	0	0	0	0	0	0	0	0	0	0	0
Obstruction	0	0	0	0	0	0	0	0	0	1	1	1	1
Misappropriation	0	0	0	0	0	0	0	0	0	0	0	0	0
Misuse	0	0	0	0	0	0	0	0	0	0	0	0	0
Level of Threat	100%	100%	100%	97%	100%	100%	97%	97%	97%	85%	85%	85%	85%

Table 31. Evaluated Potential of Threat Actions (Example)

1. Natural Threats

The mobile base stations, enhanced Wi-Fi, tethered tactical, and sleeve approaches are inherently mobile as opposed to the other fixed infrastructure approaches. Increased network mobility (i.e., on-the-move, portable, fix, etc.) can assist in physically relocating equipment to less threatening environments and, therefore, reducing the potential of the natural threats. For example, tornadoes occur frequently in the middle of the United States. However, tornadoes are less likely to occur in Alaska. Therefore, since the mobile network devices are highly mobile the threat is inherently reduced as the location changes.

a. Service Abuse

Removing the cost of service limits the potential of service abuse from occurring. For example, cellular networks cost the end users money per minute of use.

However, assuming a Wi-Fi connection is not charged per megabyte, this approach could create an environment where the threat of service abuse does not exist.

2. Interception, Electronic Tracking, and Obstruction

The threat of a malicious agent intercepting or obstructing your data is reduced by operating in environments without these agents. For example, in Antarctica, the threat of an agent intercepting emissions is less likely (low perceived value of information) than outside of high-value national assets (high perceived value). As another example, on military bases with enforced perimeters, the physical environment is restricted to authorized personnel only. Therefore, the level of threat is limited to only internal personnel.

3. Remaining Threat Actions

Environmental threats, backdoor, spam, inference, intrusion, masquerade, falsification, misappropriation, misuse, and corruption are other types of potential threat actions that could potentially exploit vulnerabilities. None of the other approaches modifies the environment to the extent that they mitigate threats and, therefore, they are assessed to have limited to no affect on threat action. For example, spam is a threat action that is just as likely to occur regardless of network architecture, since it is low cost and low risk for the perpetrator. Since these threats are potentially reduced through management policies, the technical architectures presented in this chapter have no affect on these remaining threats.

B. VULNERABILITIES

Table 22 lists security controls (from Appendix A) that potentially limit vulnerabilities in the rows, and the columns list the various architectures being evaluated. The average of the scores for each network represents the total vulnerability for the list in the table.

	Commercial MNO (Retail)	Commercial MNO w/ MCEP	RAN (only edge network)	Enhanced WiFi (Garrison)	Customer Service, Sales, Billing	Integrated VM and Messaging	Edge Network w/ Commercial Core	Core Network w/ Edge Network	DoD MNO	Mobile Base Station	Enhanced WiFi (Tactical)	Tethered Tactical Networks	Tactical Waveform Sleeve
Management Controls	0	1	0	1	1	1	1	2	2	1	1	2	2
Operational Controls	0	1	0	0	1	1	1	1	1	0	0	2	2
Identification & Authentication	0	2	0	0	2	2	2	2	2	1	0	2	2
Authorization	0	2	0	0	2	2	2	2	2	0	0	0	0
Access Controls Enforcement	1	1	0	0	1	1	1	1	1	0	0	2	2
Nonrepudiation	0	0	0	0	0	0	0	0	0	0	0	0	0
Protected Communications	1	2	1	2	2	2	2	2	2	2	2	2	2
Transaction Privacy	1	2	0	0	2	2	2	2	2	0	0	0	0
Audit Trail Maintenance	0	0	0	0	1	1	1	1	1	0	0	0	0
Protection of Server Resident Data	0	0	0	0	0	0	0	1	1	0	0	2	2
Level of Vulnerability	85%	45%	95%	85%	40%	40%	40%	30%	30%	80%	85%	40%	40%

Table 32. Vulnerability Metrics

The most vulnerable network operation approaches in Table 22 are RAN, commercial MNO, and Wi-Fi network access points. This is attributed to the use of standard commercial communication protocols. The other approaches implement additional controls to reduce vulnerability.

The MVNO concepts provide organizational structure to facilitate additional controls. For example, the DoD currently has multiple contracts and agreements spread across hundreds of commands, agencies, and departments. The lack of centralized control limits the DoD's ability to implement device and expense management systems. According to the characteristics the systems provide, and the authors' ranking of those potential system controls, the resulting score is greatly reduced from the current commercial approach.

The least vulnerable approach is the DoD's owning and controlling a separate core and edge mobile network. Assuming the ownership of the core network increases the operational, management, and technical controls, then these approaches should result in a lower vulnerability.

C. IMPACT AND OVERALL RISK

Impact and the resulting risk for each architecture would be calculated in the same way as in Chapter IV, in accordance with the guidance from NIST (2002).

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- ABI Research. (2010, August 25). Custom data cut. Oyster Bay, NY.
- Avotus. (2006). *Manage your mobile and wireless spend: A “how to” guide for the enterprise*. Murray Hill, NJ: Author.
- Brill Worldwide Investments. (2010). *Communications and Technology Solutions Wireless Cost Management*. Blue Bell, PA: Author.
- Brodkin, J. (2010). A look at bare-metal hypervisor basics. *Network World*, 27(14), 11. Retrieved from EBSCOhost.
- Boettcher, C., DeLong, R., Rushby, J., & Sifre, W. (2008). The MILS component integration approach to secure information sharing. *Digital Avionics Systems Conference, 2008. DASC 2008. IEEE/AIAA 27th*, pp. 1.C.2.1-1.C.2.14. Retrieved from IEEE Xplore.
- Business Monitor International, Ltd. (2010). Company profiles. *USA Telecommunications Report, Q1 2010*, 71–86. Retrieved from EBSCOhost.
- Business Monitor International, Ltd. (2010). Market Data Analysis. *United States Telecommunications Report Q4 2010*, 25–69. Retrieved from EBSCOhost.
- Carson, P. (2008). iPhone virtual teardown: Apple margin beats 50%. *RCR Wireless News*, 27(20), 7. Retrieved from EBSCOhost.
- Chiarelli, G. P. (2009). *MEMORANDUM: Achieving Army network and battle command modernization objectives*. Washington, DC: Office of the Vice Chief of Staff.
- Christensen, C. (1997). *The innovator’s dilemma*. Boston, MA: Harvard Business School Press.
- CTIA-The Wireless Association. (2010a). *Wireless Glossary of Terms Q-S*. Retrieved from <http://www.ctia.org/advocacy/research/index.cfm/AID/10406>
- CTIA-The Wireless Association. (2010b). *Wireless Glossary of Terms L-M*. Retrieved from <http://www.ctia.org/advocacy/research/index.cfm/AID/10408>
- CTIA-The Wireless Association. (2010c). *CTIA semi-annual wireless industry survey*. Retrieved from <http://www.ctia.org/advocacy/research/index.cfm/AID/10316>
- Compton, P. (2010). *Federal Acquisition—Key issues and guidance*. Vienna, VA: Management Concepts Inc.

- Committee on National Security Systems (2010). *National Information Assurance (IA) glossary* (CNSSI No. 4009). Retrieved from <http://www.cnss.gov/instructions.html>
- Datamonitor. (2010a). *Company profile: Research in Motion Limited*. Retrieved from EBSCOhost.
- Datamonitor. (2010b). *Wireless telecommunication services industry profile: United States (2010)*. Retrieved from EBSCOhost.
- Datamonitor. (2010c). *Mobile phones industry profile: United States*. Retrieved from EBSCOhost.
- Defense Information Systems Agency. (2010). *DISN data services*. Retrieved December 22, 2010, from DISA Services and Capabilities: <http://www.disa.mil/services/data.html>
- Defense Procurement News. (2010, March 16). *MIDS JTRS receives NSA certification - Press release*. Retrieved April 30, 2010, from <http://www.defenseprocurementnews.com/2010/03/16/mids-jtrs-receives-nsa-certification-press-release/>
- Department of Defense. (2009, August 19). Dictionary of military and associated terms. *Joint Publication 1-02*. Washington, DC: Department of Defense.
- Department of Defense. (2010, June). DoD FY11 budget request summary justification. Washington, DC: Department of Defense.
- Department of Defense. (2011, February). FY2012 budget briefing. Retrieved from <http://comptroller.defense.gov/budget.html>
- Department of the Navy Research, Development & Acquisition. (n.d.). *MUOS mobile user objective system*. Retrieved Jan 2010, from https://acquisition.navy.mil/rda/home/programs/information_communications/muos
- Dixon, J. (2010). *Integrating cellular handset capabilities with marine corps tactical communications*. M.S. thesis, Acquisition Research Program. Monterey, CA: Naval Postgraduate School.
- Edwards, C. (2010). HP gets its hands on Palm. *Bloomberg Businessweek*, 4177, 35. Retrieved from EBSCOhost.
- Federal Communications Commission. (n.d.). Auction 73 results. Available from <https://auctionsignon.fcc.gov/signon/index.htm>

- Federal Communications Commission. (2008, March 20). Auction 73: 700MHz band fact sheet. Retrieved from http://wireless.fcc.gov/auctions/default.htm?job=auction_factsheet&id=73
- Federal Communications Commission. (2009, 10 February). Auction 73. Retrieved February 15, 2011, from 700 MHz band: http://wireless.fcc.gov/auctions/default.htm?job=auction_summary&id=73
- Federal Communications Commission. (2010, December 1). Auction 66. Retrieved February 15, 2011, from Advanced Wireless Services (AWS-1): http://wireless.fcc.gov/auctions/default.htm?job=auction_summary&id=66
- Federal Communications Commission. (2010a). *Trends in telephone service*. Retrieved from <http://www.fcc.gov/wcb/iatd/trends.html>
- Federal Communications Commission. (2010b). *Wireless competition report, fourteenth report*. Retrieved from http://wireless.fcc.gov/index.htm?job=cmrs_reports
- Feintuch, J., & Spira, J. (2005, Dec.) *The cost of not paying attention: How interruptions impact knowledge worker productivity..* New York, NY: Basex.
- General Dynamics C4 Systems. (2010). Sectera Edge Smartphone (SME PED) - Cost-effective SIPRNET on the Move. Needham, MA.
- Geroski, P., & Vlassopoulos, T. (1991). The rise and fall of a market leader: Frozen foods in the U.K. *Strategic Management Journal*, 12(6), 467–478. Retrieved from EBSCOhost.
- Global Industry Analysts, Inc. (2010). *Smartphones: A global strategic business report*. San Jose, CA: Global Industry Analysts, Inc.
- Goodness, E., & Redman, P. (2010, December). *Magic quadrant for telecom expense management*. Stamford, CT: Gartner, Inc.
- Hewlett Packard. (n.d.). Valuetronics. *Signal analyzers—Spectrum analyzers, high-performance portable—HP 8560A, 8561B, 8562A, 8563*.
- International Data Corporation. (2010, June). Worldwide Smartphone 2010–2014 Forecast Update. Framingham, MA: International Data Corporation.
- International Data Corporation. (2011). *Top-selling smartphones in the U.S. in the fourth quarter*. Retrieved from <http://www.fiercewireless.com/pages/top-selling-smartphones-u-s-fourth-quarter>
- Internet Engineering Task Force. (2000). *Internet Security Glossary*. Retrieved from <http://www.ietf.org/rfc/rfc2828.txt>

- IVENT, r. a. (2008). *Creating your own private GSM network*. Netherlands: Chief Research and Innovation Centre.
- IVENT/RIC. (2010). *GSM business case NLD MoD GSM network*. Unknown Location: Support Command Ministry of Defence.
- Jacobides, M. G. (2005). Industry change through vertical disintegration: How and why markets emerged in mortgage banking. *Academy of Management Journal*, 48(3), 465–498. Retrieved from EBSCOhost.
- Jaspers, F., Hulsink, W., & Theeuwes, J. (2007). Entry and innovation in maturing markets: Virtual operators in mobile telecommunications. *Technology Analysis & Strategic Management*, 19(2), 205–225. Retrieved from EBSCOhost.
- Joint Program Executive Office Joint Tactical Radio System. (2005, August). *JPEO JTRS Overview to OMB*. Retrieved Jan 2010 from <http://jpeojtrs.mil>
- JPEO JTRS. (2010). *Appropriation / Budget Activity*. San Diego, CA: Research, Development, Test & Evaluation, Navy.
- JPEO JTRS, Financial Office. (2010). *Appropriation / Budget Activity*. San Diego: Navy.
- Katz, M. L., & Shapiro, C. (1985). Network externalities, competition, and compatibility. *American Economic Review*, 75(3), 424. Retrieved from EBSCOhost.
- L-3 Communications Systems-East. (2008, April 24). L3 Guardian SME PED - L-3 Guardian Briefing. Camden, NJ: L-3 Communications Systems-East
- Lampson, B. W. (1973). A Note on the Confinement Problem. USA, Xerox Palo Alto Research Center.
- Levin, T., Irvine, C., & Nguyen, T. (2006). *An analysis of three kernel-based multilevel security architectures*. Monterey, CA: Naval Postgraduate School.
- Lin, Yu-Chieh (2003). Value network and business strategy for mobile data: The mobile data markets in Korea, Japan, the United Kingdom, and the United States. M.A. thesis, Michigan State University, United States—Michigan. Retrieved from ABI/INFORM Global.
- Llamas, R. T., & Stofega, W. (2010). *Worldwide smartphone 2010–2014 forecast update: June 2010*. Framingham, MA: International Data Corporation.
- Luallen, M. E., & Hamburg, S. E. (2010). Control system security perceptions and practices: *Control Engineering*, 57(1), 46–48. Retrieved from ABI/INFORM Global.

- Luna, L. (2010). Security threats to smart phones jump in 2010. *Urgent Communications: Online Exclusive*. Retrieved from ProQuest.
- MarketsandMarkets, Inc. (2010). *Global Smartphones Market*. Dallas, TX: MarketsandMarkets.
- Maryland Procurement Office. (2010). *Amendment of Solicitation / Modification of Contract*. Fort Meade: National Security Agency.
- Mankiw, N. G. (2006). *Essentials of Economics*, 4th Ed. Mason, OH: South-Western Cengage Learning.
- Mazmanian, M., Yates, J. & Orlikowski, W. (2006, August). Ubiquitous e-mail individual experiences and organizational consequences of blackberry use. 65th *Annual Meeting of the Academy of Management*. Atlanta, GA.
- Mergent, Inc. (2008). American Tower Corporation. Available from <http://www.mergentonline.com>
- MindCommerce. (2010). *MVNO Niche or Boom: Data, Telemetry, and M2M MVNOs*. Superior, CO: MindCommerce.
- McNally, D., Wakefield, T., Mayne, A., & Bowler, D. (2007). *Introduction to Mobile Communications: Technology, Services, Markets*. DOI: 10.1201/9781420046540
- Mobile Phone News. (1993, November 8). Bellsouth, IBM unveil personal communicator phone. Orlando, FL: Mobile Phone News.
- Morgan Stanley. (2009). *The mobile internet report setup* [PDF document]. Retrieved from http://www.morganstanley.com/institutional/techresearch/mobile_internet_report122009.html
- Moro, T. (2007). *Analyzing the Return on Investment of a Blackberry Deployment*. New York, NY: Ipsos Reid.
- NAIP Program Office. (2010). *Assurance continuity—green hills software INTEGRITY-178B separation kernel, comprising: INTEGRITY-178B Real Time Operating System (RTOS)*. Retrieved August 31, 2010 from <http://www.niap-ccevs.org/st/vid10119/maint200/>
- National Institute of Standards and Technology (NIST). (1995). *Special Publication 800-12: An introduction to computer security: The NIST handbook* [PDF document]. Available from <http://www.nist.gov/publication-portal.cfm>

- National Institute of Standards and Technology (NIST). (2002). *Special Publication 800-30: Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology* [PDF document]. Available from <http://www.nist.gov/publication-portal.cfm>
- National Institute of Standards and Technology (NIST). (2008). *Special Publication 800-124: Guidelines on Cell Phone and PDA Security* [PDF document]. Available from <http://www.nist.gov/publication-portal.cfm>
- Navy Marine Corps Internet (NMCI). (2010). *NMCI to GFE cellular phone services migration: Process & CLIN overview*. NMCI.
- Network Strategy Partners (2009). *The business case for RAN backhaul using mobile transport over packet*. Concord, MA: Network Strategy Partners, LLC.
- The NPD Group. (2009, March 3). *Despite recession, U.S. smartphone market is growing: Smartphones gain share against all other handsets in 2008, as prices become more competitive*. Retrieved from http://www.npd.com/press/releases/press_090303.html
- Nunez, R. (2010, September 7). OK Labs forging the mobile virtualization movement. *The Huffington Post*. Retrieved from http://www.huffingtonpost.com/ramon-nunez/ok-labs-forging-the-mobil_b_707499.html
- Office of the Director of National Intelligence. (2007). *Intelligence Community Directive Number 700*. Retrieved from http://www.dni.gov/electronic_reading_room.htm
- Office of Management and Budget. (2007). *Commercial Spectrum Enhancement Act*. Washington, DC: Office of Management and Budget.
- Pagani, M., & Fine, C. H. (2008). Value network dynamics in 3G-4G wireless communications: A systems thinking approach to strategic value assessment. *Journal of Business Research*, 61(11), 1102–1112.
- Peppard, J., & Rylander, A. (2006). From Value Chain to Value Network: Insights for Mobile Operators. *European Management Journal*, 24(2/3), 128–141.
- Porter, M. E. (2008). The Five Competitive Forces That Shape Strategy. *Harvard Business Review*, 86(1), 78–93. Retrieved from EBSCOhost.
- Pressley, T. (2010, December). Advantages of LTE for the Warfighter. Reston, V: Ericsson.
- Pyramid Research. (2009, December). *Smartphone Forecast: Operator strategies will fuel growth in emerging markets*. Cambridge, MA: Pyramid Research.

- Quickcomm, STS International, Visage Mobility Central. (2010). *Controlling wireless expenses: Has logic gone out the window*. Hyoun Park: Aberdeen Group.
- Reed, B. (2010). The BlackBerry will win. *Network World*, 27(2), 24–27. Retrieved from EBSCOhost.
- Research In Motion, Limited. (2011). BlackBerry security. Retrieved from <http://us.blackberry.com/ataglance/security>
- Red Bend Software. (2011). *Mobile virtualization: How it works*. Retrieved from http://www.redbend.com/index.php?option=com_content&view=article&id=133%3Amobile-virtualization-how-it-works&catid=33&Itemid=61&lang=en
- Sabat, H. K. (2003). Delivering mobile wireless value through the evolving value chain. *IIMB Management Review (Indian Institute of Management Bangalore)*, 15(1), 42–54. Retrieved from EBSCOhost.
- Smith, S. (2010). *Worldwide smartphone sales forecast to 2015*. Guildford, United Kingdom: Coda Research Consultancy.
- Sprint. (2010). Sprint Store. Retrieved August 31, 2010, from Shop Phones: <http://shop.sprint.com/NASApp/onlinestore/en/Action/DisplayPhones?phoneSKU=MOT1KIT>
- Suh, S. (2007). Secure Xen on ARM: Status and driver domain separation [PDF document]. Presented at Xen Summit, November 2007. Retrieved from <http://wiki.xensource.com/xenwiki/XenARM>
- Telberg, R. (2007). *The connected accountant: The growing mobility trend*. Dobbs Ferry, NY: Bay Street Group.
- TerraNet. (2010). *TerraNet Solutions*. Retrieved March 2010, from TerraNet AB: <http://www.terranet.se>
- Tutorials Point (2011). WiMAX–Reference network model. Retrieved from <http://www.TutorialsPoint.com>
- Uchenick, G., & Vanfleet, W. M. (2005) “Multiple independent levels of safety and security: high assurance architecture for MSLS/MLS” *Military Communications Conference, 2005*. Vol. 1, 17–20.
- U.S. Census Bureau. (2010, June 1). *Government Employment & Payroll*. U.S. Census Bureau. Retrieved August 28, 2010, from: <http://www.census.gov/govs/apes/>

- Vane, L. M. (2009). *MEMORANDUM: Battle Command and Network Segment Objectives for Capability Set 13–14*. Headquarters United States Army Training and Doctrine Command, Army Capabilities Integration Center. Fort Monroe: Office of the Assistant Secretary of the Army (Acquisition, Logistics and Technology).
- Virtualization.info. (2008). *Is virtualization ready to go mobile?* Retrieved from <http://virtualization.info/en/news/2008/06/is-virtualization-ready-to-go-mobile.html>
- Ware, W. H. (1970). *Security controls for computer systems: Report of Defense Science Board Task Force on Computer Security*. Santa Monica, CA: The RAND Corporation.
- Whalley, J., & Li, L. (2002). Deconstruction of the telecommunications industry: From value chains to value networks. *Telecommunications Policy*, 26, 451–472.
- White, A. (2010, July 17). *How Mobile Virtual Network Aggregators (MVNA) Have Changed the Financing of a MVNO*. Available from <http://ezinearticles.com>
- White, H. (2009). *MVNO operational cost planning: Modeling and negotiation strategies for contracting with host mobile network operators*. Superior, CO: MindCommerce.
- White, H. (2010). *U.S. Mobile Virtual Network Operators 2010: The Definitive Guide and Critical Analysis of the U.S. MVNO Market*. Superior, CO: MindCommerce.
- Wildavsky, A., & Wildavsky, A. (2008). Risk and safety In D. R. Henderson (Ed.), *The concise encyclopedia of economics*. Retrieved from <http://www.econlib.org/library/Enc/RiskandSafety.html>

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Marine Corps Representative
Naval Postgraduate School
Monterey, California
4. Director, Training and Education
MCCDC, Code C46
Quantico, Virginia
5. Director, Marine Corps Research Center, MCCDC, Code C40RC
Quantico, Virginia
6. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
Camp Pendleton, California
7. Grant Wagner
National Security Agency
Fort Meade, Maryland
8. Mary Berlage
National Security Agency
Fort Meade, Maryland
9. Gerry Zuelsdorf
National Security Agency
Fort Meade, Maryland
10. Marine Corps Systems Command, PG11
Quantico, Virginia
11. Information Assurance Directorate
National Security Agency
Fort Meade, Maryland

12. Nicholas Dew
Naval Postgraduate School
Monterey, California
13. John Dillard
Naval Postgraduate School
Monterey, California
14. Cynthia Irvine
Naval Postgraduate School
Monterey, California